JP9-1999-0.

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

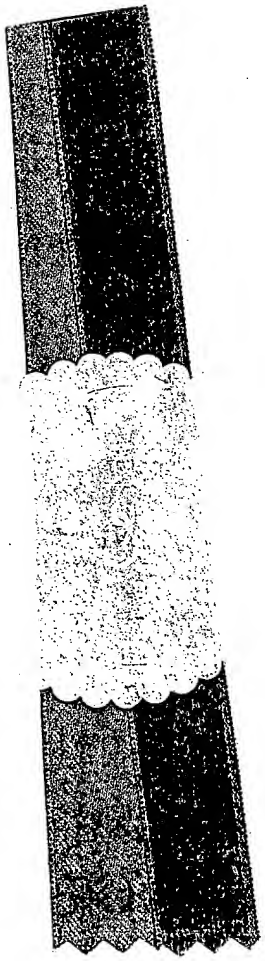
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年　６月２９日

出 願 番 号
Application Number: 特願２０００－１９６３９６

出 願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレーション



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月２２日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号　出証特２０００－３１０７２８９

【書類名】　特許願

【整理番号】　JA999241

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 17/22

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　立花　隆輝

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　清水　周一

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　小林　誠士

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　中村　大賀

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【連絡先】　０４６－２１５－３３１８、３３２５、３４５５

【選任した代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【選任した代理人】

【識別番号】　100106699

【弁理士】

【氏名又は名称】　渡部　弘道

【手数料の表示】

【予納台帳番号】　024154

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0004480

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】電子透かし方法およびそのシステム

【特許請求の範囲】

【請求項１】

デジタルデータに付加情報を埋め込む、電子透かしシステムであって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該システムが、

（１）デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換部と、

（２）周波数領域変換部において得られたデジタルデータの周波数成分の振幅を、付加情報のビット情報と、前記周波数成分の周波数帯により増減する、周波数領域埋め込み部と、

（３）周波数領域埋め込み部で得られた、振幅を増減された周波数成分を、逆フーリエ変換を使って時間領域の信号へと戻す、時間領域変換部と、

（４）時間領域変換部で得られた時間領域の信号に、窓関数を乗じ、重なり合う前後のフレームを重ね合わせて、付加情報の埋め込まれたフレームを作成する、付加情報埋め込みフレーム作成部

を有する、電子透かしシステム

【請求項２】

前記周波数領域埋め込み部（２）が、デジタルデータの周波数成分の振幅を、付加情報のビット情報と、周波数帯に対応して周波数成分を増やすのか減らすのかを予め規定したマスクの値により増減する、請求項１記載のシステム。

【請求項３】

１つの周波数帯に含まれるすべての周波数に対応する前記マスクの値をすべて等しくすることを特徴とする、請求項２記載のシステム。

【請求項４】

前記周波数帯の幅を高周波の周波数ほど広くすることを特徴とする、請求項２～３記載の何れかに記載のシステム。

【請求項５】

付加情報の埋め込まれた、デジタルデータから、該付加情報を検出する電子透かし検出システムであって、

（１）デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換部と

（２）周波数領域変換部において得られた周波数成分から振幅を求め、該振幅を所定のフレーム数分だけ蓄積する、振幅蓄積部と、

（３）振幅蓄積部において蓄積された振幅値に基づき、ビット検出の開始とすべき検出開始フレームを特定する、サイクル同期部と、

（４）サイクル同期部において得られた検出開始フレームから、埋め込まれた付加情報のビット情報を検出する、ビット検出部

を有する、電子透かし検出システム。

【請求項６】

前記周波数領域変換部（１）において、前記フレームの長さを、埋め込みをしたときの長さよりも短くすることを特徴とする、請求項５記載のシステム。

【請求項７】

前記サイクル同期部（３）が、蓄積された振幅値から検出開始フレームを特定するにあたり、周波数成分を加えるのか減じるのかを予め規定したマスクの値を用いた演算結果に基づき、検出開始フレームを特定する、請求項５記載のシステム。

【請求項８】

デジタルデータに付加情報を埋め込む、電子透かし方法であって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該方法は、

（１）デジタルデータから１フレームを現フレームとして取り出す段階と、

（２）前記取り出した現フレームに、既定の窓関数を乗じる段階と、

（３）前記窓関数を乗じた現フレームにフーリエ変換を行い、現フレームの周波数成分を求める段階と、

（４）付加情報のビット情報に応じて、前記周波数成分の振幅を変更する段階と、

（５）前記変更された周波数成分を、逆フーリエ変換する段階と、

（６）前記逆フーリエ変換された、前記変更された周波数成分に、前記窓関数を乗じる段階と

（７）上記（１）～（６）と同様の段階で既に処理された前フレームの後ろからＮ－Ｍサンプルと、上記（６）の段階で処理された現フレームの頭からＭサンプルを足し和せ、新しいＮ個のサンプルからなる１フレームを作成する段階を有する、電子透かし方法。

【請求項９】

前記周波数成分の振幅を変更する段階（４）が、付加情報のビット情報と、周波数帯に対応して周波数成分を増やすのか減らすのかを予め規定したマスクの値により振幅を増減する、請求項８記載の方法。

【請求項１０】

１つの周波数帯に含まれるすべての周波数に対応する前記マスクの値をすべて等しくすることを特徴とする、請求項９記載の方法。

【請求項１１】

前記周波数帯の幅を高周波の周波数ほど広くすることを特徴とする、請求項９～１０記載の何れかに記載の方法。

【請求項１２】

付加情報の埋め込まれた、デジタルデータから、該付加情報を検出する方法であって、

（１）デジタルデータから、Ｎサンプルからなる１フレームを取り出す段階と、

（２）前記取り出したフレームに、既定の窓関数を乗じる段階と、

（３）前記窓関数を乗じたフレームにフーリエ変換を行い、該フレームの周波数成分を求める段階と、

（４）前記周波数成分の振幅の値を蓄積する段階と、

（５）上記（１）～（４）の段階を、前記蓄積が既定の量に達した場合、付加情報検出のための最適な開始フレームを算出する段階と、

（６）前記開始フレームから、埋め込まれた付加情報のビット情報を検出する段階

を有する、付加情報検出方法。

【請求項１３】

前記１フレームを取り出す段階（１）において、該フレームの長さを、埋め込みをしたときの長さよりも短くすることを特徴とする、請求項１２記載のシステム。

【請求項１４】

前記最適な開始フレームを算出する段階（５）が、蓄積された振幅の値から開始フレームを特定するにあたり、周波数成分を加えるのか減じるのかを予め規定したマスクの値を用いた演算結果に基づき、開始フレームを算出する、請求項１２記載の方法。

【請求項１５】

デジタルデータに付加情報Ｎ(≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータから、Ｒ（Ｒ≧１）サンプル目までサンプル値を読み取る段階と

（２）デジタルデータから、（Ｒ＋１）以降のサンプル値を読み取る段階と、

（３）前記取り出した（Ｒ＋１）以降のサンプル値を付加情報のビット情報に応じて変更する段階と、

（４）デジタルデータのＲサンプルと前記付加情報のビット情報に応じて変更された（Ｒ＋１）サンプル以降を足し和せる段階

を有する、電子透かし方法。

【請求項１６】

デジタルデータに付加情報Ｎ(≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータからサンプル値を読み取る段階と、

（２）前記取り出したサンプル値を付加情報のビット情報に応じて変更するにあたり、該付加情報の先頭ビット以外から、付加情報のビット情報に応じて変更を

開始する段階と、

（３）前記変更されたサンプル値から、新しいデジタルデータを作成する段階

を有する電子透かし方法。

【請求項１７】

デジタルデータに付加情報Ｎ(≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータからサンプル値を読み取る段階と、

（２）前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、

（３）前記変更されたサンプル値に、ランダムにノイズを付加する段階と、

（４）前記変更されたサンプル値から、新しいデジタルデータを作成する段階

を有する電子透かし方法。

【請求項１８】

デジタルデータに付加情報Ｎ(≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータからサンプル値を読み取る段階と、

（２）前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階であって、該変更を行わない場合を、ランダムに設ける段階と、

（３）前記変更されたサンプル値、およびは変更されないサンプル値から、新しいデジタルデータを作成する段階

を有する電子透かし方法。

【請求項１９】

デジタルデータに付加情報Ｎ(≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータの特定のサンプルを重複、挿入、削除、シフトして、デジタルデータを変更する段階と、

（２）デジタルデータからサンプル値を読み取る段階と、

（３）前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、

（４）前記変更されたサンプル値から、新しいデジタルデータを作成する段階
を有する電子透かし方法。

【請求項２０】

デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータを時間軸上で伸縮する段階と、

（２）デジタルデータからサンプル値を読み取る段階と、

（３）前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、

（４）前記変更されたサンプル値から、新しいデジタルデータを作成する段階
を有する電子透かし方法。

【請求項２１】

デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータからサンプル値を読み取る段階と、

（２）前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、

（３）前記変更されたサンプル値から、新しいデジタルデータを作成する段階

（４）新しいデジタルデータを時間軸上で伸縮する段階

を有する電子透かし方法。

【請求項２２】

前記伸縮の伸縮率が１％以内である、請求項２０乃至２１記載の何れかに記載の電子透かし方法。

【請求項２３】

デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータをサンプリング周波数 r’ でリサンプリングして、サンプル値を読み取る段階と、

（２）前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階

であって、

（３）前記変更されたサンプル値を、元のサンプリング周波数 ｒ でサンプリングして新しいデジタルデータを作成する段階

を有する電子透かし方法。

【請求項２４】

デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって

（１）デジタルデータをサンプリング周波数 ｒ’ でサンプリングして、サンプル値を読み取る段階と、

（２）前記取り出したサンプル値に対して、付加情報のビット情報に応じた変更量を求める段階と、

（３）前記求められた変更量を、元々のデジタルデータのサンプリング周波数 ｒ でリサンプリングする段階と、

（４）元々のデジタルデータに、前記リサンプリングされた変更料を加え、新しいデジタルデータを作成する段階

を有する電子透かし方法。

【請求項２５】

デジタルデータに、付加情報を埋め込むプログラムを含むコンピュータ読み取り可能な記録媒体であって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該プログラムがコンピュータに、

（１）デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換機能と、

（２）周波数領域変換部において得られたデジタルデータの周波数成分の振幅を、付加情報のビット情報と、前記周波数成分の周波数帯により増減する、周波数領域埋め込み機能と、

（３）周波数領域埋め込み部で得られた、振幅を増減された周波数成分を、逆フーリエ変換を使って時間領域の信号へと戻す、時間領域変換機能と、

（４）時間領域変換部で得られた時間領域の信号に、窓関数を乗じ、重なり合う

前後のフレームを重ね合わせて、付加情報の埋め込まれたフレームを作成する、付加情報埋め込みフレーム作成機能
を実現させる、コンピュータ読み取り可能な記録媒体。

【請求項２６】

付加情報の埋め込まれたデジタルデータから、該付加情報を検出するプログラムを含むコンピュータ読み取り可能な記録媒体であって、該プログラムがコンピュータに、

（１）デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換機能と、

（２）周波数領域変換部において得られた周波数成分から振幅を求め、該振幅を所定のフレーム数分だけ蓄積する、振幅蓄積機能と、

（３）振幅蓄積部において蓄積された振幅値に基づき、ビット検出の開始とすべき検出開始フレームを特定する、サイクル同期機能と、

（４）サイクル同期部において得られた検出開始フレームから、埋め込まれた付加情報のビット情報を検出する、ビット検出機能
を実現させる、コンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】

本発明はデジタルデータに対する電子透かし技術に関し、特に実用的かつ堅牢な電子透かし技術に関する発明である。

【０００２】

【従来の技術】

従来の電子透かし技術では、理論上における電子透かし方法を単にそのまま製品に応用した範疇を出ておらず、真に実用的な、また埋め込みアルゴリズムを解析不能にする電子透かし技術を提供していない。デジタルデータへの電子透かし技術の例として、周波数空間で埋め込み・検出を行う方法に米国特許 5687236 がある。従来の周波数空間における電子透かし方法は埋め込まれた情報（付加情報）を検出する際、埋め込みの開始を示す情報（埋め込み開始情報）に同期するよ

うにして付加情報の検出を行っている。しかしながら、このような方法では、本来の埋め込むべき情報と別に同期のための信号を埋め込む必要があり、付加情報を検出するにはまず該同期信号を検出しなければならず、当然それにかかる時間も必要となる。また悪意のある第３者により同期信号を検出された場合に埋め込まれた付加情報が容易に解析、抽出される危険性がある。したがって、実用的でかつ堅牢な電子透かしの技術が望まれる。

【０００３】

【課題を解決するための手段】

本発明の課題は、このような従来の電子透かしにおける欠点に鑑み、実用的かつ堅牢な電子透かしの方法およびシステムを提供することである。

また別の課題は、埋め込まれた付加情報の検出に用いる、同期信号を必要としない、電子透かし方法およびシステムを提供することである。

また別の課題は、埋め込まれた付加情報の検出時間を低減する、電子透かし方法およびシステムを提供することである。

また別の課題は、埋め込みアルゴリズムの解析を困難にする、電子透かし方法およびシステムを提供することである。

【０００４】

【課題を解決するための手段】

本発明は前記課題を解決するために、以下の手段を採用した。

デジタルデータに付加情報を埋め込む、電子透かしシステムであって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該システムが、デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換部と、周波数領域変換部において得られたデジタルデータの周波数成分の振幅を、付加情報のビット情報と、前記周波数成分の周波数帯により増減する、周波数領域埋め込み部と、周波数領域埋め込み部で得られた、振幅を増減された周波数成分を、逆フーリエ変換を使って時間領域の信号へと戻す、時間領域変換部と、時間領域変換部で得られた時間領域の信号に、窓関数を乗じ、重なり合う

前後のフレームを重ね合わせて、付加情報の埋め込まれたフレームを作成する、付加情報埋め込みフレーム作成部を有する。

【０００５】

好適には、前記周波数領域埋め込み部が、デジタルデータの周波数成分の振幅を、付加情報のビット情報と、周波数帯に対応して周波数成分を増やすのか減らすのかを予め規定したマスクの値により増減する。#d

好適には、１つの周波数帯に含まれるすべての周波数に対応する前記マスクの値をすべて等しくする。

【０００６】

好適には、前記周波数帯の幅を高周波の周波数ほど広くする。

【０００７】

また別の態様として、付加情報の埋め込まれた、デジタルデータから、該付加情報を検出する電子透かし検出システムであって、デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換部と、周波数領域変換部において得られた周波数成分から振幅を求め、該振幅を所定のフレーム数分だけ蓄積する、振幅蓄積部と、振幅蓄積部において蓄積された振幅値に基づき、ビット検出の開始とすべき検出開始フレームを特定する、サイクル同期部と、サイクル同期部において得られた検出開始フレームから、埋め込まれた付加情報のビット情報を検出する、ビット検出部を有する。

【０００８】

好適には、前記周波数領域変換部において、前記フレームの長さを、埋め込みをしたときの長さよりも短くする。

【０００９】

好適には、前記サイクル同期部が、蓄積された振幅値から検出開始フレームを特定するにあたり、周波数成分を加えるのか減じるのかを予め規定したマスクの値を用いた演算結果に基づき、検出開始フレームを特定する。

【００１０】

また別の態様として、デジタルデータに付加情報を埋め込む、電子透かし方法で

あって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該方法は、デジタルデータから１フレームを現フレームとして取り出す段階と、前記取り出した現フレームに、既定の窓関数を乗じる段階と、前記窓関数を乗じた現フレームにフーリエ変換を行い、現フレームの周波数成分を求める段階と、付加情報のビット情報に応じて、前記周波数成分の振幅を変更する段階と、前記変更された周波数成分を、逆フーリエ変換する段階と、前記逆フーリエ変換された、前記変更された周波数成分に、前記窓関数を乗じる段階と、同様の段階で既に処理された前フレームの後ろからＮ－Ｍサンプルと、現フレームの頭からＭサンプルを足し和せ、新しいＮ個のサンプルからなる１フレームを作成する段階を有する。

【００１１】

好適には、前記周波数成分の振幅を変更する段階が、付加情報のビット情報と、周波数帯に対応して周波数成分を増やすのか減らすのかを予め規定したマスクの値により振幅を増減する。

【００１２】

好適には、１つの周波数帯に含まれるすべての周波数に対応する前記マスクの値をすべて等しくする。

【００１３】

好適には、前記周波数帯の幅を高周波の周波数ほど広くする。

【００１４】

また別の態様として、付加情報の埋め込まれた、デジタルデータから、該付加情報を検出する方法であって、デジタルデータから、Ｎサンプルからなる１フレームを取り出す段階と、前記取り出したフレームに、既定の窓関数を乗じる段階と、前記窓関数を乗じたフレームにフーリエ変換を行い、該フレームの周波数成分を求める段階と、前記周波数成分の振幅の値を蓄積する段階と、前記蓄積が既定の量に達した場合、付加情報検出のための最適な開始フレームを算出する段階と、前記開始フレームから、埋め込まれた付加情報のビット情報を検出する段階を有する。

【００１５】

好適には、前記１フレームを取り出す段階において、該フレームの長さを、埋め込みをしたときの長さよりも短くする。

【００１６】

好適には、前記最適な開始フレームを算出する段階が、蓄積された振幅の値から開始フレームを特定するにあたり、周波数成分を加えるのか減じるのかを予め規定したマスクの値を用いた演算結果に基づき、開始フレームを算出する。

【００１７】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータから、Ｒ（Ｒ≧１）サンプル目までサンプル値を読み取る段階とデジタルデータから、（Ｒ＋１）以降のサンプル値を読み取る段階と、前記取り出した（Ｒ＋１）以降のサンプル値を付加情報のビット情報に応じて変更する段階と、デジタルデータのＲサンプルと前記付加情報のビット情報に応じて変更された（Ｒ＋１）サンプル以降を足し和せる段階を有する。

【００１８】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータからサンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更するにあたり、該付加情報の先頭ビット以外から、付加情報のビット情報に応じて変更を開始する段階と、前記変更されたサンプル値から、新しいデジタルデータを作成する段階を有する。

【００１９】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータからサンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、前記変更されたサンプル値に、ランダムにノイズを付加する段階と、前記変更されたサンプル値から、新しいデジタルデータを作成する段階を有する。

【００２０】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータからサンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階であって、該変更を行わない場合を、ランダムに設ける段階と、前記変更されたサンプル値、およびは変更されないサンプル値から、新しいデジタルデータを作成する段階を有する。

【００２１】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータの特定のサンプルを重複、挿入、削除、シフトして、デジタルデータを変更する段階と、デジタルデータからサンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、前記変更されたサンプル値から、新しいデジタルデータを作成する段階を有する。

【００２２】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータを時間軸上で伸縮する段階と、デジタルデータからサンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、前記変更されたサンプル値から、新しいデジタルデータを作成する段階を有する。なお好適には前記伸縮の伸縮率は１％以内である。

【００２３】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータからサンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、前記変更されたサンプル値から、新しいデジタルデータを作成する段階と、新しいデジタルデータを時間軸上で伸縮する段階を有する。なお好適には前記伸縮の伸縮率は１％以内である。

【００２４】

また別の態様として、デジタルデータに付加情報Ｎ（≧１）ビットを埋め込む、

電子透かし方法であって、デジタルデータをサンプリング周波数 r' でリサンプリングして、サンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階であって、前記変更されたサンプル値を、元のサンプリング周波数 r でサンプリングして新しいデジタルデータを作成する段階を有する。

【００２５】

また別の態様として、デジタルデータに付加情報N（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータをサンプリング周波数 r' でサンプリングして、サンプル値を読み取る段階と、前記取り出したサンプル値に対して、付加情報のビット情報に応じた変更量を求める段階と、前記求められた変更量を、元々のデジタルデータのサンプリング周波数 r でリサンプリングする段階と、元々のデジタルデータに、前記リサンプリングされた変更料を加え、新しいデジタルデータを作成する段階を有する。

【００２６】

また別の態様として、デジタルデータに付加情報N（≧１）ビットを埋め込む、電子透かし方法であって、デジタルデータをサンプリング周波数 r でサンプリングして、サンプル値を読み取る段階と、前記取り出したサンプル値を付加情報のビット情報に応じて変更する段階と、前記変更されたサンプル値から、新しいデジタルデータを作成する段階と、前記新しいデジタルデータをサンプリング周波数 r' でサンプリングして、サンプル値を読み取る段階と、前記サンプル値から、より新しいデジタルデータを作成する段階を有する。

【００２７】

また別の態様として、デジタルデータに、付加情報を埋め込むプログラムを含むコンピュータ読み取り可能な記録媒体であって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該プログラムがコンピュータに、デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換機能と、周波数領域変換部において得られたデジタルデータの周波数成分の振

幅を、付加情報のビット情報と、前記周波数成分の周波数帯により増減する、周波数領域埋め込み機能と、周波数領域埋め込み部で得られた、振幅を増減された周波数成分を、逆フーリエ変換を使って時間領域の信号へと戻す、時間領域変換機能と、時間領域変換部で得られた時間領域の信号に、窓関数を乗じ、重なり合う前後のフレームを重ね合わせて、付加情報の埋め込まれたフレームを作成する、付加情報埋め込みフレーム作成機能を実現させる。

【００２８】

また別の態様として、付加情報の埋め込まれたデジタルデータから、該付加情報を検出するプログラムを含むコンピュータ読み取り可能な記録媒体であって、該プログラムがコンピュータに、デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換機能と、周波数領域変換部において得られた周波数成分から振幅を求め、該振幅を所定のフレーム数分だけ蓄積する、振幅蓄積機能と、振幅蓄積部において蓄積された振幅値に基づき、ビット検出の開始とすべき検出開始フレームを特定する、サイクル同期機能と、サイクル同期部において得られた検出開始フレームから、埋め込まれた付加情報のビット情報を検出する、ビット検出機能を実現させる。

【００２９】

【発明の実施の形態】

以下、本発明の実施の形態を図１～図２２の図面に基いて説明する。実施例の説明において使用される用語の定義を表１に、また記号一覧を表２に示す。なお、本実施例はデジタルデータへの電子透かしの例としてデジタルオーディオデータにおける電子透かしの方法およびシステムについて説明するが、実施の形態としては、デジタル動画像データ（ＭＰＥＧなど）についても全く同様に実施できることはいうまでもない。

【表１】

DFT	Discrete Fourier Transform。離散フーリエ変換。 デジタルオーディオデータの周波数成分を求める処理。
FFT	Fast Fourier Transform。高速離散フーリエ変換。 離散フーリエ変換を高速で行うアルゴリズムである。 本明細書中でFFTとしているところは他のDFTにしても同じ結果が得られるが 処理にかかる時間が長くなる。
IFFT	Inverse Fast Fourier Transform。逆高速離散フーリエ変換。
時間領域	FFTを行う前の、デジタルオーディオデータのPCM波形がある空間。
周波数領域	デジタルオーディオデータにFFTを行った後の周波数成分がある空間。
フレーム	本発明の埋め込み・検出システムは、デジタルデータから一定サンプル数を 取り出してFFTを行う。 その一定サンプル数で構成されるデジタルデータを１フレームと呼ぶ。
窓	本発明では、埋め込みや検出でFFTを行う前やIFFTを行った後のデジタルデータに ある関数を乗じる。この処理を「窓をかける」といい、かける関数を「窓関数」と いう。基本的に窓関数としてはサイン関数を用いるが、条件を満たす関数であれば 他の関数でも構わない。
付加情報	デジタルデータに埋め込む、著作権情報、複製・再生許諾条件、曲名、歌詞などの 情報。 それらの情報はまず１と０のビット列として表現し、さらに０を－１に置き換えて から実際の埋め込みに使う。
原 音	埋め込みが行われていないデジタルオーディオデータ。
埋め込み信号	埋め込みの時にデジタルデータを増減するその変化分の信号。 時間領域でも周波数領域でも同じこの用語を用いる。
周波数帯	本発明では全周波数帯をいくつかの周波数帯に分け、それぞれに１ビットを埋める。 (例外もあり。)
マスク	埋め込みシステムと検出システムの両方が了解している＋１と－１の列。 埋め込みの時にデジタルデータの周波数成分を増やすか減らすかを 規定する。検出の時にも周波数成分を加えるか引くかをこれが規定する。
フレーム同期	従来の周波数空間検出では必要だったが、本発明の検出では必要のない処理。 埋め込みの時にデジタルデータのどこからどこまでをフレームとして 埋め込みが行われたかを調べる処理。
ビット検出値	検出の時に、デジタルデータに埋まっている付加情報の各ビットを 判定するのに使う数値。
サイクル同期	本発明の検出で行う処理のひとつ。先頭のフレームを決定する処理。
フレームずれ	検出の時に最初にFFTしたフレームと、埋め込みをしたときに先頭だったフレームが 何フレームずれているかの量。検出時の最初には不明。

【表２】

N	１フレームに含まれるサンプル数。
n	何番目のサンプルなのかを表すのに用いるインデクス。正負の整数をとる。
B	埋め込む付加情報のビット数。
b	何番目のサンプルなのかを表すのに用いるインデクス。０以上の自然数をとる。
W	埋め込みに用いる周波数の数。
w	何番目の周波数なのかを表すインデクス。W以下の自然数をとる。
F	１回の埋め込みに用いるフレームの数。
f	何番目のフレームなのかを表すインデクス。F以下の自然数をとる。
a(f,n)	デジタルオーディオデータのフレームｆのｎ番目のサンプル値。 重ね合わせがあるので a(f+1,n) ≡ a(f,n+N/2)である。 (0＜n ≦N/2) 埋め込み後については a'(f,n)を用いることもある。
aw(f,n)	デジタルオーディオデータに窓をかけた後の、フレームｆの ｎ番目のサンプル値。埋め込み後については aw'(f,n)を用いることもある。
w(n)	窓関数。
lower(b)	ｂ番目のビットを埋め込む周波数帯の中で最小の周波数。
upper(b)	ｂ番目のビットを埋め込む周波数帯の中で最大の周波数。
CB	埋め込む付加情報の配列。CB_bで構成される。
CB_b	埋め込む付加情報のｂ番目の値。＋１か−１の値をとる。
C	埋め込む付加情報の配列。周波数を添字に使う。
C_w	周波数ｗに埋め込む付加情報の値。＋１か−１の値をとる。
M	マスクの行列。Ｆ行Ｗ列。
$M_{f,w}$	フレームｆ，周波数ｗでのマスク。＋１か−１の値をとる。 $M_{f,w}(C)$の略記として使うこともある。
$M_{f,w}(C)$	付加情報Ｃを埋めるのに用いる、フレームｆ，周波数ｗでのマスク。 ＋１か−１の値をとる。
$F_{f,w}$	フレームｆ，周波数ｗの周波数成分ベクトル。実数成分と虚数成分を持つ。
$F'_{f,w}$	埋め込みを行った後の周波数成分ベクトル。
$F_{f,w}$	フレームｆ，周波数ｗの振幅。埋め込み後についてF'を用いることもある。
$I_{f,w}$	フレームｆ，周波数ｗの虚数成分。埋め込み後についてI'を用いることもある。
$R_{f,w}$	フレームｆ，周波数ｗの実数成分。埋め込み後についてR'を用いることもある。 $F_{f,w} = \lvert F_{f,w} \rvert = \sqrt{R_{f,w}^2 + I_{f,w}^2}$ の関係がある。
$\Delta F_{f,w}$	フレームｆ，周波数ｗの埋め込み信号。周波数空間におけるベクトル表現。 $F'_{f,w} = F_{f,w} + \Delta F_{f,w}$である。
$\Delta I_{f,w}$	フレームｆ，周波数ｗの埋め込み信号の虚数成分。 $I'_{f,w} = I_{f,w} + \Delta I_{f,w}$である。
$\Delta R_{f,w}$	フレームｆ，周波数ｗの埋め込み信号の実数成分。 $R'_{f,w} = R_{f,w} + \Delta R_{f,w}$である。
$P_{f,w}$	フレームｆ，周波数ｗについて、聴覚心理モデルで求めた許容範囲。
C_b	ｂ番目の付加情報についての検出値。浮動小数点数。
$C_b(s)$	ｓフレームだけずれていると仮定した場合の、ｂ番目の付加情報についての検出値。
$C_{+,b}$	ｂ番目の付加情報に−１が埋まっていると仮定して求めた検出値。浮動小数点数。
$C_{-,b}(s)$	ｓフレームずれを仮定した場合の、$C_{+,b}$。
$C_{-,b}$	ｂ番目の付加情報に−１が埋まっていると仮定して求めた検出値。浮動小数点数。
$C_{-,b}(s)$	ｓフレームずれを仮定した場合の、$C_{-,b}$。
S_s	ｓフレームずれを仮定した場合のサイクル同期の値。浮動小数点数。
T_b	ビットの信頼性を判断するための閾値。あらかじめ設定しておく定数。
TWM	透かしの有無を判断するための閾値。あらかじめ設定しておく定数。

【００３０】

＜第１の実施の形態＞

デジタルオーディオデータに対する実用的かつ堅牢な電子透かしの第１の実施例として、デジタルオーディオデータに対するフレーム同期の必要がない電子透かしの方法およびシステムについて説明する。

【００３１】

埋め込みシステムは以下の機能からなる。

（１）周波数領域変換部

・サンプルの取り出し

入力されたデジタルオーディオデータからNサンプルを取り出す。

・窓がけ

取り出したデジタルオーディオデータに窓関数を乗じる。

・FFT

FFTを行い周波数成分を求める。

（２）周波数領域埋め込み部

周波数領域変換部において得られた周波数成分の振幅を、付加情報のビット情報と、周波数成分の周波数帯により増減する。周波数成分に聴覚心理モデルを適用し、変更しても人の耳には違いのわからない許容範囲を算出し、その許容範囲だけ、デジタルオーディオデータの周波数成分を増減する。

（３）時間領域変換部

変更後の周波数成分にIFFTを行う。周波数領域埋め込み部で得られた、振幅を増減された周波数成分を、逆フーリエ変換を使って時間領域の信号へと戻す。

（４）付加情報埋め込みフレーム作成部

時間領域変換部で得られた時間領域の信号に、窓関数を乗じ、重なり合う（隣り合う）前後のフレームを重ね合わせて、付加情報の埋め込まれたフレームを作成する。

【００３２】

検出システムは以下の機能からなる。

（１）周波数領域変換部

・サンプルの取り出し

入力されたデジタルオーディオデータからNサンプルを取り出す。

・窓がけ

取り出したデジタルオーディオデータに窓関数を乗じる。

・FFT

FFTを行い周波数成分を求める。

（２）振幅蓄積部

周波数成分から振幅を求め、該振幅を所定のフレーム数分だけ蓄積する。

（３）サイクル同期部

振幅蓄積部において蓄積された振幅値に基づき、ビット検出の開始とすべき開始フレームを特定する。周波数領域検出部において得られた検出値を所定のフレーム数分だけ保存し、蓄積された検出値において、最も検出値の絶対値が大きい値を探し、これをフレームずれとして出力する。つまりどのフレームを先頭にしてビット検出をするべきかのフレームずれを求める。

（４）ビット検出部

サイクル同期部において得られた検出開始フレームから、埋め込まれた付加情報のビット情報を検出する。サイクル同期で求めたフレームずれに基づいて各ビットを検出し、出力する。

【００３３】

図１に、本発明の実用的で堅牢な電子透かしの埋め込み方法のフローチャートを示す。

まずステップ１１０で、入力データであるデジタルデータから１フレーム（Ｎサンプル）を取り出す。次にステップ１２０で、取り出したフレームに窓関数を乗じる。そしてステップ１３０で、窓関数を乗じたフレームにフーリエ変換をほどこす。これによりフレームの周波数成分が求まる。次にステップ１４０で、周波数領域に変換されたフレームの周波数成分を、位相を保つようにしつつ、付加情報に応じて振幅を増減する。この時、振幅を増加させるか減少させるかはそのフレームに埋める付加情報のビット情報と、そのフレームのその周波数帯(バンド)に対応するマスクの符号によって決定される。また振幅を増減させる量は、心理

聴覚モデル部において決められた変更量を用いる。なおこの変更量については、入力であるデジタルデータに対して、増減しても人間には音質の変化がわからない、変更量が計算される。次にステップ１５０で、埋め込みが完了した周波数成分(振幅を増減された周波数成分)を、逆フーリエ変換し、時間領域の信号へと戻す。そしてステップ１６０で得られた時間領域の信号に再び、窓をかける。最後に前のフレームと重ねあわせて付加情報の埋め込まれたフレームを作成する。

【００３４】

図２に、本発明の実用的で堅牢な電子透かしの検出方法のフローチャートを示す。

まずステップ２１０で、入力データであるデジタルデータから１フレーム（Ｎサンプル）を取り出す。次にステップ２２０で、取り出したフレームに窓関数を乗じる。そしてステップ２３０で、窓関数を乗じたフレームにフーリエ変換をほどこす。これによりフレームの周波数成分が求まる。次にステップ２４０で、周波数領域に変換されたフレームの周波数成分を所定のフレーム数分だけ保存する。所定のフレーム数分だけ蓄積したら、最も検出値の絶対値が大きい場所を探し、それをフレームずれ(ユニットの先頭位置)として出力する。この計算は所定のマスクを用いた演算によりなされ、あるフレームを先頭位置と仮定した検出値が求まる。最後にステップ２６０で、得られたフレームずれからの検出値を選び、その値と周波数の大小により埋め込まれた付加情報のビット情報を決定する。

【００３５】

[標準的な埋め込み・検出方法]

本発明の埋め込み・検出手法の詳細な流れについて説明する。

【００３６】

[埋め込む付加情報]

まず準備として埋め込む付加情報を記号で表す。埋め込む付加情報は1と0のビット列である。そのうちすべての0を-1で置き換えて並べた配列を作る。

【数１】

$$CB = |CB_1, CB_2, \ldots, CB_b, \ldots, CB_B|$$
$$= |+1, +1, \ldots, -1, \ldots, +1|$$

本手法はこの付加情報の各ビットをある幅を持った周波数帯に割り当てる。

【数２】

$$C_w = CB_b \qquad (lower(b) \leq w \leq upper(b))$$

上の式は b 番目のビットが lower(b) から upper(b) までの周波数を持つ周波数帯に割り当てられ、その範囲の周波数に埋める情報 C_w はすべて CB_b とするということを表している。ビットと周波数帯の対応はどのフレームでも変わらない。図３はフレーム軸（時間軸）と周波数軸が直行することと、ある周波数帯には常に同じビットが埋められていることを表現した図である（塗りつぶしの模様が同じ部分は同じビットを表わす）。

【００３７】

［マスク］

マスクは +1 と -1 の行列である。埋め込みシステムと検出システムは同じマスクを了解している必要がある。その意味でマスクは一種の秘密鍵としての役割を果たす。埋め込みシステムにとってはマスクは、それぞれの周波数成分を増やすのか減らすのかを規定するものである。検出システムにとってのマスクは検出式中でそれぞれの周波数成分を加えるのか減じるのかを規定するものである。

【数３】

$$M = \begin{bmatrix} M_{1,1}(C_1) & \cdots & M_{1,W}(C_W) \\ \vdots & M_{f,w}(C_w) & \vdots \\ M_{F,1}(C_F) & \cdots & M_{F,W}(C_W) \end{bmatrix}$$

【００３８】

［サンプルの取り出し］

時間順に並んだデジタルオーディオデータからNサンプルを取り出す。取り出したフレーム f の n 番目のサンプルを a(f,n) と表記する。この N サンプルは処理の単位でありフレームと呼ぶ。あるフレームとそれに連続するフレームは半分重なる。図４はフレームの重なりを説明する図である。

【００３９】

［窓がけ］

フレームに対して FFT をかける際には窓関数を乗じる。基本的にはサイン関数が適しているが、下式の性質を満たすものであれば他の関数でもよい。これは窓を 2度かけて重ね合わせた時に埋め込みなければデジタルオーディオデータが復元されるということを保証する。

【数４】

$$w(n)^2 + w(n+N/2)^2 = 1$$

ここで n は N/2 以下の自然数である。サイン窓は

【数５】

$$w(n) = \sin\left(\pi \frac{n}{N}\right)$$

である。窓をかけるという操作は下式の通り。

【数６】

$$aw(f,n) = w(n) \times a(f,n)$$

ここで n は N 以下の自然数である。

【００４０】

[FFT]

aw(f,n) に FFT をかけて周波数成分 $F_{f,w}$ を得る。

【００４１】

[パワー埋め込み]

埋め込みでは位相を変えずに振幅（パワー）のみを増減する。

図５は振幅の増減を説明する図である。

【数７】

$$F'_{f,w} = F_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

$$I'_{f,w} = I_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

$$R'_{f,w} = R_{f,w} \times \left\{ 1 + M_{f,w}(C_w) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

【００４２】

[IFFT]

埋め込んだ周波数成分 $F'_{f,w}$ に IFFT をかけ、aw'(f,n) を得る。

【００４３】

[窓をかけ、重ね合わせて時間順に出力]

再び窓関数を乗じ、連続するフレームと足し合わせ出力すればデジタルオーディオデータへの埋め込みは完成する。

【数８】

$$a'(f,n) = \begin{cases} w(n) \times aw'(f,n) + w(n+N/2) \times aw'(f-1,n+N/2) & (0<n\leq N/2) \\ w(n) \times aw'(f,n) + w(n-N/2) \times aw'(f+1,n-N/2) & (N/2<n\leq N) \end{cases}$$

上式は、フレームの前半分は前のフレームと足し合わせ、後半分は後ろのフレームと足し合わせることを意味している。左辺が埋め込み後のデジタルオーディオデータでありこれを出力すればこのフレームfについての埋め込みは終わる。図６は窓かけとフレームの重ねあわせを説明する図である。

【００４４】

[サイクル同期]

検出の処理のうちFFTをかけ周波数成分を求めるまでは埋め込みの処理と同じである。その後、各周波数の振幅 $F_{f,w}$ を求めてバッファに記憶しておく。フレームFまで溜ったらサイクル同期とビット検出をすることができる。ここで、デジタルオーディオデータの一部が切り取られているかもしれないので、f=1は必ず

しも埋め込みの時に先頭だったフレームだとは限らない。フレームがずれているとマスクとそれと乗じる振幅が食い違うので正しくビット検出をすることができない。図７はフレームずれのない場合であり、図８は１フレームずれている場合である。サイクル同期はフレームずれｓを仮定してS_sを求めこれを最大にするｓを求める操作である。図９はサイクル同期を説明する図である。ｓは０から（F-1）までのすべての整数について試す。S_sを求める式は、ビット検出値の和である。まずフレームずれｓを仮定したビット０（すなわち埋め込みの時にはC_wが-1だった)のビット検出式は、

【数９】

$$c_{-,b}(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w}(-1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

であり、ビット1（すなわち埋め込みの時にはがC_{w+1}だった)に対するビット検出式は

【数１０】

$$c_{+,b}(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w}(+1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

である。ここでマスク$M_{f+s,w}(c)$の一つ目の添字（f+s）はmod Fで用いる。これを正しいビットについて合計したものがサイクル同期の検出式である。しかしｂ番目のビットが+1だったのか-1だったのか不明であるので、大きい方を選び合計する。

【数１１】

$$S_s = \sum_{b=1}^{B} max\{c_{-,b}(s), c_{+,b}(s)\}$$

このS_sを最大にする s がフレームずれの答えである。

【００４５】

［ビット検出］

ビット検出は、サイクル同期で求めたフレームずれ s を用い、$C_{-,b(s)}$ と $C_{+,b(s)}$ の大小を比較することでビットを判定する。

【数１２】

$$b\text{番目のビット} = \begin{cases} 1 & (c_{+,b}(s) > c_{-,b}(s)) \\ 0 & (c_{+,b}(s) < c_{-,b}(s)) \end{cases}$$

【００４６】

［バリエーション］

以下に基本的な埋め込み・検出システムの性能をあげるための拡張手法や代替方法を説明する。

【００４７】

［透かしの閾値・ビットの閾値］

デジタルオーディオデータ中に透かしが埋め込まれているかどうかを判断するのには、サイクルシンクの結果求まったフレームずれ s を用いてたとえば下式で判定できる。

【数１３】

$$\text{透かし} \begin{cases} \text{有り} \left(\frac{1}{\sqrt{B}} \sum_{b=1}^{B} max\{c_{-,b}(s), c_{+,b}(s)\} > TWM \right) \\ \text{無し } otherwise \end{cases}$$

ＴＭＷはあらかじめ設定しておいた定数の閾値である。ある程度高音以上の周波数帯に埋めたビットの検出値は無視するように上式のΣの上限を下げた方がよいこともある。また、各ビットごとに検出結果が信頼できるかどうかを判定することもできる。

【数１４】

$$b\text{番目のビット} = \begin{cases} 1 & (c_{+,b}(s) - c_{-,b}(s) > T_b) \\ 0 & (c_{-,b}(s) - c_{+,b}(s) > T_b) \\ \text{信頼できるビット情報無し} & otherwise \end{cases}$$

T_b は b 番目のビットのための閾値である。この閾値はビットごとに違う定数を用いて、特に信頼性が求められるビットの閾値を高く設定するなどの使い方をしてもよい。

【００４８】

［連続する何フレームかに同じマスクで埋める］

連続する何フレームかに同じマスクで埋め込んでおくと、重なり合うフレーム同士で埋め込み信号が強め合い検出効率がよくなる。連続するフレームに同じマスクで埋めることにする。

【００４９】

［周波数を2本ずつセットにする］

検出式、数式９及び数式１０の分母を分子に対して小さくすることができれば検出値を大きくすることができる。そのひとつの方法が2本の周波数ごとセットにしてその差を分母にする方法である。埋める時はマスクの奇数周波数とそれに続く偶数周波数のマスクの符号を必ず逆にしておく。ただし w は W/2 以下の任意の自然数。f はＦ以下の任意の自然数である。検出する時は2本ずつ差をとって検出する。

【数１５】

$$c_b = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=\frac{lower(b)}{2}}^{\frac{upper(b)}{2}} M_{f,2w-1}(F_{f,2w-1} - F_{f,2w})}{\sqrt{\sum_{w=\frac{lower(b)}{2}}^{\frac{upper(b)}{2}} (F_{f,2w-1} - F_{f,2w})^2}} \right]$$

【００５０】

［マスクを2つに分解し計算を高速化］

以上の方法ではサイクル同期の際にフレームずれを０から（F-1）まで試して、その F 回の試行について毎回数式９及び数式１０を計算しなければならなかった。そこでマスクを下式のように2つのマスクの積にしておく。

【数１６】

$$M_{f,w} = MF_f \times MW_w$$

このマスクを使って埋めておけば、検出式は

【数１７】

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w} F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

$$= \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[MF_{f+s} \frac{\sum_{w=lower(b)}^{upper(b)} MW_w F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

となり、この式は

【数１８】

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} [MF_{f+s} \times q_{b,f}]$$

$$q_{b,f} = \frac{\sum_{w=lower(b)}^{upper(b)} MW_w F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}}$$

に分解することができる。この $q_{b,f}$ の方はフレームずれ s に依存しないのでサイクル同期を始める前にあらかじめ計算しておくことができる。また $F_{f,q}$ はバッファに記憶しておかなくてよいので必要な記憶容量も減る。

【００５１】

［周波数帯の幅を変え、各ビットの信頼性を差別化する］

埋め込まれる付加情報としては著作権に関する情報、複製・再生許諾情報、曲名、歌詞などの情報が考えられるが、その情報の種類によって重要性は大きくことなる。たとえば複製・再生許諾情報は曲名よりも一般に重要であり強い耐性を持つことが望ましい。本発明の手法では各周波数帯の幅を変えることで各ビットの信頼性に差別をもうけることができる。周波数帯の幅とは upper(b)-lower(b)+1 であり、これを大きくすればそのビットの耐性は強くなり信頼性も上がる。図１０は付加情報の半分をより重要な情報であるとして広い周波数帯を割り当てた例である。

【００５２】

[各ビットの信頼性を均等にする]

付加情報の各ビットが同等の信頼性を持たなければならない場合を考える。音声圧縮技術やラジオ放送など、バンドパスフィルターとしての効果がある劣化処理に対して、各ビットが同等の信頼性を持たなければならない場合にはここまでの方法では問題がある。なぜならばたとえばローパスフィルターをかけられた場合、高周波数帯に埋めたビットだけが大きく劣化してしまう。そこですべてのビットをすべての周波数帯にまんべんなくばらまかれて埋められるようにする。たとえばフレーム f ，周波数 w に埋める付加情報を下式のように決めて、ビットを斜めに埋める。

【数１９】

$$C_{f,w} = CB_b \qquad (lower(b-f+1) \le w \le (upper(b-f+1))$$

上式の lower(b-f-1) および upper(b-f-1) の括弧内は mod B である。この式が表す各ビットが埋められる位置は図１１に示す通りである。図１１で同じ模様で塗りつぶされている四角（周波数・フレーム平面での埋められる位置を表している)は同じビットを運ぶ部分である。C_w を $C_{f,w}$ としたのでマスクも $M_{f,w}(C_{f,w})$ となる。

【数２０】

$$M = \begin{bmatrix} M_{1,1}(C_{1,1}) & \cdots & M_{1,W}(C_{1,W}) \\ \vdots & M_{f,w}(C_{f,w}) & \vdots \\ M_{F,1}(C_{F,1}) & \cdots & M_{F,W}(C_{F,W}) \end{bmatrix}$$

埋め込みは

【数２１】

$$F'_{f,w} = F_{f,w} \times \left\{ 1 + M_{f,w}(C_{f,w}) \times \frac{P_{f,w}}{F_{f,w}} \right\}$$

検出するときは

【数２２】

$$c_{+,b} = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} M_{f,w}(+1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} (F_{f,w})^2}} \right]$$

$$c_{-,b} = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} M_{f,w}(-1) \times F_{f,w}}{\sqrt{\sum_{w=lower(b+f-1)}^{upper(b+f-1)} (F_{f,w})^2}} \right]$$

上式の lower(b+f−1) および upper(b+f−1) の括弧内は mod B である。ここではビットを埋める位置を規則的に斜めに埋める手法を説明したが、埋める位置が斜めに並ぶ必要はない。たとえば埋め込みの時に秘密鍵を用いて埋める位置を決

定し、検出する時にも秘密鍵から検出に用いる周波数成分の位置を知って検出をするようにもできる。そうすれば秘密鍵を知らない者には検出ができない様な仕組みをこの部分にも実装することができる。

【００５３】

［信頼性の差別化と均等化］

さらにバンドパスフィルターに対するある程度の耐性をどのビットにも持たせつつ、信頼性の差別化をすることもできる。ひとつの方法は図１２のように lower(b) および upper(b) をフレームごとに変化するようにする。すなわちこれは lower(f,b), upper(f,b) へと拡張することを意味する。埋め込み・検出システムの両方が lower(f,b), upper(f,b) を了解していればどのような値であるかは問題ではない。図１２中では再び斜め方向に同じビットが埋まるようにしているが必ずしもこのようにする必要はない。このとき付加情報の配列は

【数２３】

$$C_{f,w} = CB_b \qquad (lower(f,b) \le w \le (upper(f,b))$$

とし、ビット検出式も

【数２４】

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(f,b)}^{upper(f,b)} M_{f+s,w} \times F_{f,w}}{\sqrt{\sum_{w=lower(f,b)}^{upper(f,b)} (F_{f,w})^2}} \right]$$

とする。

【００５４】

［信頼性の差別化・均等化と高速化］

次に処理の高速化の方法を説明する。upper(f,b) と lower(f,b) に以下の制約を課す。

・周波数帯の幅 upper(f,b)-lower(f,b)+1 は何種類かに限定する。

・ビットを埋め込む位置は周波数帯の幅が同じビット同士でのみ入れ換えを行う

。

図１３は、高速化可能な斜め埋めを説明する図である。たとえば図１３では周波数帯幅を2種に限定し、信頼性の低くてもよいビットは幅が狭い周波数帯いくつかの中で斜めに埋めている一方、高い信頼性の要求されるビットは幅が広い周波数帯で斜めに埋めている。

【００５５】

［マスクの正負を使って付加情報を埋める場合］

以上の方法はビット1を埋めるマスクとビット 0 を埋めるマスクを別にしていたが、ひとつのマスクの正負でビットを区別して埋めることもできる。マスクは１つになる。

【数２５】

$$M = \begin{bmatrix} M_{1,1} & \cdots & M_{1,W} \\ \vdots & M_{f,w} & \vdots \\ M_{F,1} & \cdots & M_{F,W} \end{bmatrix}$$

埋め込みの時はビットによって増減を決める。

【数２６】

$$F'_{f,w} = F_{f,w} \times \left(1+M_{f,w} \times \frac{P_{f,w}}{F_{f,w}}\right)$$

$$I'_{f,w} = I_{f,w} \times \left(1+M_{f,w} \times \frac{P_{f,w}}{F_{f,w}}\right)$$

$$R'_{f,w} = R_{f,w} \times \left(1+M_{f,w} \times \frac{P_{f,w}}{F_{f,w}}\right)$$

サイクル同期およびビット判定の検出式はひとつになり、

【数２７】

$$c_b(s) = \frac{1}{\sqrt{F}} \sum_{f=1}^{F} \left[\frac{\sum_{w=lower(b)}^{upper(b)} M_{f+s,w} F_{f,w}}{\sqrt{\sum_{w=lower(b)}^{upper(b)} (F_{f,w})^2}} \right]$$

この式の値として正負両方が出てくるようになる。ここでマスク $M_{f+s,w}$ の一つ目の添字は mod F で用いるものとする。サイクル同期の時には絶対値をとってから合計した以下の値の最大値を求めることになる。

【数２８】

$$S_s = \sum_{b=1}^{B} | C_b(s) |$$

ビットの判定は検出値の正負で判定する。

【数２９】

$$\text{b番目のビット} = \begin{cases} 1 & (c_b(s) > 0) \\ 0 & (c_b(s) < 0) \end{cases}$$

【００５６】

[時間領域に戻してから埋め込み]

節に示した埋め込み手順を以下のように変更すれば窓がけや FFT に伴う誤差を少なくすることができる。

（１）サンプルの取り出し

（２）窓がけ

（３）FFT

（４）埋め込み信号の作成

周波数成分に聴覚心理モデルを適用し、変更しても人の耳には違いのわからない許容範囲を算出する。その範囲で、埋め込み信号を作る。

（５）IFFT

埋め込み信号にIFFTを行う。

（６）窓をかけ、重ね合わせて時間軸上に戻す。

これに窓関数を乗じ、隣り合うフレームと重ね合わせれば時間領域での埋め込み信号が得られる。

（７）デジタルオーディオデータに加える。

それを元のデジタルオーディオデータに加えれば、埋め込み後のデジタルオーディオデータとなる。それを出力する。

【００５７】

なお（４）においては、以下の式に従って埋め込み信号を作成する。

【数３０】

$$\Delta F_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{F_{f,w}}{F_{f,w}}$$

$$\Delta I_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{I_{f,w}}{F_{f,w}}$$

$$\Delta R_{f,w} = M_{f,w}(C_w) \times P_{f,w} \times \frac{R_{f,w}}{F_{f,w}}$$

【００５８】

［同一マスクの使用］

１つの周波数帯に含まれるすべての周波数に対応するマスクをすべて等しくすることにより、オーディオデータの周波数のずれに対する耐性を持たせることができる。これは、周波数のずれにより、例えば５０００Ｈｚが５０５０Ｈｚに変化

したとき、５０００Ｈｚと５０５０Ｈｚに異なるマスク（符号）が使用されていた場合、検出に悪影響を及ぼす。しかしながら同一のマスク（符号）であればその影響がない。

【００５９】

［周波数帯の幅を周波数に応じて変化させる］

最後に、周波数帯の幅を高周波の周波数ほど広くすることによって、音楽の再生スピードの変化や、長さの伸縮などによる、周波数の全体的変化に対する耐性を持たせることができる。なぜなら、再生スピードが１０％速くなると全ての周波数が１０％高くなるので、５００Ｈｚは５５０Ｈｚに、５０００Ｈｚは５５００Ｈｚになる。よって高い周波数ほど周波数のずれは大きい。このずれにどの周波数帯も耐性を持つためには、高周波ほど周波数帯が広い必要がある。

【００６０】

［検出時のフレーム長を短くする］

検出をするときの窓の長さ（すなわちフレームの長さ）を埋め込みをしたときの窓の長さよりも短くすることによって埋め込みをしたときのフレームの端の部分の影響を弱めることができる。例えば、周波数帯で同じ符号を使っている場合、埋め込みで N サンプルを1フレームにしていたとして、検出でたとえば N/2 サンプルを１フレームとする。このようにすることで、埋め込みのときに k番の周波数に埋めた符号の影響は k/2 番で観測される。検出で N/4 サンプルを１フレームとしたら、k 番の埋め込みの影響は k/4番で観測される。これは、フーリエ変換の性質として観測のフレーム長を半分にすると、観測の周波数分解能は半分になるからである。つまり、検出をするときにマスクの符号を、フレームの長さの違いに対応するだけずらしてやれば、フレームが違っても検出をすることができる。本発明の実施例では、フレームを半分またはそれ以下で重ねあわせて符号を時間方向にも変えて埋め込んでいるが、時間的に隣接するフレームの、ある周波数帯におけるマスクの符号が異なっている場合、それらのフレームが重ね合わされた部分では、埋め込みの効果は打ち消し合わされている。（たとえば符号が”＋＋－－” では ２番目と３番目で異なる符号が埋められたフレームが重ね合わされる）上記のように短いフレーム長を使って検出をすることによって、隣

接するフレームからおよぶ影響が少ない部分に限定して検出をすることが可能になるわけである。

【００６１】

＜第２の実施の形態＞

デジタルオーディオデータに対する実用的かつ堅牢な電子透かしの第２の実施例として、付加情報の埋め込みアルゴリズムを解析困難にする電子透かしを説明する。なお以下の説明において「サンプル」との記述はオーディオを対象にした場合の表現であるが、「フレーム」と読み替えれば動画像に、「ピクセル」と読み替えれば静止画像にも適用可能である。

【００６２】

［埋め込み開始位置をランダムにする］

埋め込み前のコンテンツの先頭の R サンプルを読み飛ばして、（R+1）サンプル目から埋め込みを始める。この R は埋め込みを実行する際に決まるランダム変数である。

【００６３】

［埋め込み開始ビットやフレームをランダムにする］

複数のビットを埋め込む場合には、どのビットから埋め込むかをランダムにすることができる。これは検出器が検出をする際に、どのビットが先頭なのかを定める処理が行われる場合に限って利用可能である。その場合には先頭のビットがその処理で見つけられる筈なので、コンテンツの先頭にビットの先頭が埋め込まれていなくても構わない。あるいはその変形として次の方法も考えられる。あるサンプル数（Ｆとする）を1「単位」として、そこに一つあるいは複数のビットを埋める方法では、検出の際にその単位がどこから始まるかを見つける処理が行われるはずである。先頭が見つけられるのであるから、コンテンツの先頭と「単位」の先頭が一致している必要はない。よって「単位」の何サンプル目から埋め込みを始めるかをランダムにすることができる。図１７に埋め込み開始ユニット、図１８に仮想的な埋め込み開始位置の例を示す。

【００６４】

［ランダム・ノイズを加える］

埋め込みの際に埋め込み信号だけでなく、ランダムで計算されるノイズをもコンテンツに加える。ノイズがある程度小さければ音質にも影響を与えないようにできる。ノイズが完全にランダムであれば検出結果にも大きな悪影響を与えないことが期待できる。

【００６５】

［時々埋め込みをせずにランダム信号だけを加える］

埋め込み処理の際に、埋め込みをしないでランダム信号だけを加える部分をランダムに決めるタイミングで作る。この方法は検出結果にいくらか悪影響を与えるが、コンテンツの他の部分から検出できるのでいくらか埋め込みをしていない部分があっても構わない場合に利用できる。

【００６６】

［埋め込み前に前処理を行う］

埋め込み処理を行う前に、ランダム性を備える前処理でコンテンツを加工する。図１４は埋め込み前の前処理、埋め込み後の後処理を説明する図である。

【００６７】

処理前のコンテンツ0 → ［前処理］ → 前処理後、埋め込み前コンテンツ0’→ ［埋め込み］ → 埋め込み後コンテンツ 0’’

【００６８】

この手順を内部で行えば悪意を持ったユーザーは「前処理後、埋め込み前コンテンツ0’」を知ることができない。よって悪意をもったユーザーは「処理前のコンテンツ0」と「埋め込み後コンテンツ0’’」の差分 D = 0’’- 0 を知ることはできても、「埋め込み後コンテンツ0’’」と「前処理後、埋め込み前コンテンツ0’」の差分 D’’= 0’’- 0’ を知ることはできない。D’ には埋め込みによる効果 D と前処理による効果 D’= 0’- 0 の両方が含まれているので、埋め込みアルゴリズムの特定が困難になる。前処理の例としてはサンプルの重複・挿入・欠落、サンプルのシフト、伸縮などがある。それぞれについて説明する。

【００６９】

・［サンプルの重複・挿入・欠落］

コンテンツからランダムにサンプルを欠落させたり、あるサンプルを繰り返した

り、あるサンプルを挿入したりする。これは音楽の場合には「音程を保つ時間伸縮（pitch-preserved time expansion/compression)」と一般に呼ばれる処理であり、欠落・重複・挿入をする頻度が十分低ければ音質に影響はまったく与えない（たとえば1秒44100サンプルに1サンプル)。静止画像では水平ラインや垂直ラインを重複・挿入・欠落させることにあたる。動画像では一枚一枚の静止画像の水平ラインや垂直ラインを重複・挿入・欠落させてもよいし、静止画像（フレーム)を1単位として重複・挿入・欠落させてもよい。音質・画質に与える影響を特に小さく保つように万全を期すつもりなら、それを行う場所をコンテンツの特性を見て選ばなければならない（このことも音程を保つ時関伸縮で一般に行われている)。すなわちたとえば欠落・重複・挿入をする場所を、似通ったサンプル値が連続するところに限る、など。欠落によって減るサンプル数と、重複・挿入によって増えるサンプル数を同数になるように調節すれば、処理後のコンテンツの長さを処理前のコンテンツの長さと同じにすることができる。

【００７０】

・[サンプルのシフト]

コンテンツをランダムサンプル数だけシフトする。言いかえればコンテンツの先頭にサンプルをつけ加えたり、先頭からサンプル取り除いたりする。は必ずしも整数でなくても構わない。が整数でない実数である場合には補間によってコンテンツの各サンプル値を決めることになる。たとえば1次の線形補間を使うならば

【数３１】

$$v'(x) = ([x+r] + 1 - (x+r)) \times v([x+r]) + ((x+r) - [x+r]) \times v([x+r] + 1)$$

によってサンプル値を変更する。

ここで [r] は r を超えない最大の整数を表し、v(x) は処理前の x 番目のサンプル値を、v'(x) は処理後のx番目のサンプル値を表す。

【００７１】

・[伸縮]

ごく少ない程度であれば、コンテンツを伸縮することもここでの目的に使うこ

とができる。たとえば1%以下の線形伸縮であれば人間の耳では変化を認めることができない。この処理によってコンテンツの長さが保たれるように、ある部分は伸長して、ある部分は縮小することも可能である。 これらの方法は前処理にランダム性がなくても効果は高い。つまり、前処理が決定的なアルゴリズムであるとしても、そのアルゴリズムが知られさえしなければD''を知ることは困難である。

【００７２】

［埋め込みを行った後に後処理を行う］

埋め込み前に前処理を行う方法と同様の処理を埋め込み後のコンテンツに施すことも、埋め込み信号を解析されにくくする上では同様の効果を持つ。埋め込み信号自体も処理が加えられている点で解析されにくさは強くなっているとも言える。しかしこの処理によって埋め込み信号がいくらか劣化してしまうので、検出成績は少し悪化することが予想される。

【００７３】

［リサンプリングを行ってから埋め込み信号を計算する］

この方法は埋め込み前に前処理を行う方法と似ているが、オリジナルのコンテンツは変化させない点が異なっている。ここでいうリサンプリングは動画像・静止画像では画素数を変化させることにあたる。この方法の手順は以下の通り。図１５はリサンプリングを行ってから埋め込み信号を計算する方法を説明する図である。

【００７４】

・処理前のコンテンツ 0 のサンプリング周波数を r と仮定する。

・処理前のコンテンツ 0 をサンプリング周波数 r' へとリサンプリングし、リサンプル後のコンテンツ 0'を求める。

・リサンプル後のコンテンツ0' に対して仮埋め込み信号E'を求める。E' のサンプリング周波数も r' である。

・仮埋め込み信号E'をサンプリング周波数 r へとリサンプリングして埋め込み信号Eを求める。

・処理前のコンテンツ0 に埋め込み信号Eを加え、埋め込み後のコンテンツ0" と

する。

【００７５】

あるいは図１６（リサンプリングを行ってから埋め込み信号を計算）のように

・処理前のコンテンツ0 のサンプリング周波数を ｒ と仮定する。

・処理前のコンテンツ0 をサンプリング周波数r’ へとリサンプリングし、リサンプル後のコンテンツ0’ を求める。

・リサンプル後のコンテンツ0’ に対して仮埋め込み信号E’ を求める。E’ のサンプリング周波数も ｒ’ である。

・仮埋め込み信号E’ をリサンプル後のコンテンツ0’ に加え、サンプリング周波数 ｒ’ における埋め込み後のコンテンツ0” を作成する。

・サンプリング周波数 ｒ へとリサンプリングして埋め込み後のコンテンツ0’’’ を求める。

【００７６】

埋め込みに使ったサンプリング周波数は、埋め込み実行時にランダムで決めてもよいし、ランダムでなくてもアルゴリズムを隠す上では効果があると思われる。埋め込み信号を作る際に、基準となるサンプル数図１７、図１８でのユニット）を用いている場合に、その長さをわかりにくくすることがこの方法によって可能になる。

【００７７】

［検出結果を出力する間隔をランダムにする］

この方法は差分を解析されにくくする方法ではないが、アルゴリズムを解析されにくくする方法であるという点で他のアイディアと共通しているのでここに挙げる。この方法は、検出の際に検出結果が得られたらすぐにその結果を表示したり、コピーを止めたりするなどアクションを起こすのではなく、故意に（ランダムに決まる）ある程度の時間だけその出力を遅らせるということである。これによって検出までにかかる最小時間を悪意を持ったユーザーに知られないようにする。

【００７８】

［ビット情報埋め込み位置の時間変動］

画像またはオーディオコンテンツに電子透かしとしてＮビット（Ｎ≧１）の情報を埋め込む際、時間推移とともにビット情報埋め込み単位（以降ユニットと呼ぶ）内の各ビットの埋め込み位置を変化させる。これにより、ビット情報埋め込みコンテンツのある特定の位置が加工あるいは破壊されたとしても、ある特定のビット情報のみが検出不可あるいは改竄されることを避けることができる。また、埋まっている情報が同じであるとしても埋め込み位置が違うので、複数のコンテンツの平均をとっても埋め込み信号が強めあわなくなる。このことも電子透かしのアルゴリズムや鍵の解析を困難にする上で好ましい。ここで、時刻ｔ（ユニット番号）における番目のビット情報埋め込み位置を P(n,t) とすると、時刻 t+1 における同ビット情報埋め込み位置は、P(n,t+1)=F(P(n,t))と表すことができる。ここで、Ｆ（Ｐ）は、ビット情報埋め込み位置を変更する変換演算子とする。また、Ｐ、Ｆ（Ｐ）は、ある周期Ｔを持っている。

【数３２】

$$P(n,t+T) = F^{T}(P(n,t)) = P(n,t)$$

【００７９】

図１９は、Ｐ、Ｆ（Ｐ）の例で、1ユニット内に4ビットの情報を埋め込んむ場合の1例を示している。図１９中の大きな□はユニットを表し、ユニット内の小さな番号のふられた□はそれぞれビット情報を埋め込む位置を表しているものとする。

【００８０】

この例では、

Ｐ(n,t)= t + n　mode 4（Ｔ＝４、n=0,1,2,3)

である。Ｆ（Ｐ）を複雑に、またを長くすることにより、ビット情報埋め込み位置の推定し、ある特定ビット情報のみを検出不可にすることまたは改竄することをより困難にすることができる。

【００８１】

また、時間推移とともに、ビット情報埋め込み位置のみでなく、埋め込み情報の

解釈を変えることも可能である。この手法はまた、電子透かしを埋め込む原コンテンツが時間的に相関を持つ場合には、時間推移とともにビット情報埋め込み位置を変更しているため、原コンテンツの相関を打ち消すことができ、埋め込み情報がないにもかかわらず埋め込み情報があるとしてしまうエラー比率（false positive error ratio)を下げる効果もある。

【００８２】

［検出］

時間的にユニット内のビット情報埋め込み位置を変化させてあるので検出の際にも以下のように、ビット情報埋め込み位置変化の周期ごとに埋め込み情報の検出を行う必要がある。

【数３３】

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n,t+i)))$$

【００８３】

ここで、Ｄ（Ｐ（ｎ，ｔ））は各ユニット内の情報埋め込み位置からの電子透かしの検出演算子であり、Ｄｎはその検出値である。ここで、情報埋め込みビット数Ｎ≧２の場合には、情報を埋め込んだコンテンツが加工された際には、検出値の内、どの位置からの検出値が、情報埋め込み時の先頭のビットを表しているのかが分からなくなるため、情報埋め込み時の先頭ビット位置を検出する必要が出て来る。その方法を以下に説明する。

【００８４】

情報埋め込みビット数Ｎ≧２の場合には、情報埋め込み時の先頭ビット位置が検出値Ｄｎのうちどれにあたるかを以下のいずれかの方法で検出する。

【００８５】

［情報を埋め込まない位置の挿入］

ビット情報埋め込み位置変更周期Ｔの際、埋め込み情報とは別に同じＴの周期で何も情報を埋め込まない場所を先頭埋め込みビットを検出するための目印として

挿入しておく。たとえば、図１９のＰ、Ｆ（Ｐ）の例では、例えば図２０のように情報を埋め込まない部分を挿入しておく。図２０中の黒く塗られた部分がフレーム内で情報を埋め込まない場所であるとする。検出時には、情報を埋め込んだ位置の検出値が、|Ｄｎ|＞Ｔｈを満たすとすると、min(|Ｄｎ|)＜Ｔｈとなるｎ番目の検出値を埋め込み情報の先頭を得るための目印として得ることができる。ただしＴｈはある閾値である。

【００８６】

[周期２Ｔでビット反転する情報の埋め込み]

ビット情報埋め込み位置変更周期Ｔの際、埋め込み情報とは別にＴの周期でビット反転する情報を埋め込んでおく。図２１は周期２Ｔでビット反転する情報の埋め込み例を示す図である。図２１中の＋あるいはーが周期Ｔでビット反転する情報を表わしているものとする。検出時には、２Ｔの周期で数式３３に基づいて各検出を算出し、

【数３４】

$$D0_n \cdot D1_n < 0$$

となるｎ番目の検出値を見ることで、埋め込み情報の先頭を得ることができる。ここで、

【数３５】

$$D0_n = \sum_{i=0}^{T-1} D(F^i(P(n,t+i)))$$

$$D1_n = \sum_{i=T}^{2T-1} D(F^i(P(n,t+i)))$$

である。

【００８７】

［ビット情報以外の情報の利用］

埋め込みビットの先頭を検出する際に、他の信号の検出値を用いる。例えば電子透かし検出用に、ユニットの位置決め情報（シンク情報）が埋まっている場合には、ビット情報埋め込み時に、その信号の符号を埋め込み位置変更周期Ｔ毎に反転させる。あるいは、周期Ｔ毎に符号が反転した部分を挿入する。これによって、検出時には、位置決め情報の符号の変化する部分をみることで、埋め込みビットの先頭位置を検出することができる。図２２はビット情報以外の情報の利用例を示す図である。

【００８８】

［埋め込み情報の解釈変更］

あるビットを繰り返しコンテンツに埋め込む場合、特定の符号列に応じて部分部分ごとに反転させて埋め込む。常に同じ情報が埋め込まれているのではなくなるので、解析しにくくなる。ある時点で埋め込む情報は以下の式で計算する。

【数３６】

$$B'(t) = B \times M(t)$$

【００８９】

ここで、Ｂは本来のビット情報（１か－１かの値をとる。ビットは０か－１で表現する）、Ｂ’（ｔ）はコンテンツの時間推移に応じて反転されたビットであり、これが実際にはコンテンツに埋め込まれる。Ｍ（ｔ）は埋め込み情報を反転させる符号列であり、＋１か－１の値をとる。このように、時間推移とともに、埋め込み情報の解釈を変えたい場合には、各検出値Ｄｎを得る際に、

【数３７】

$$D_n = \sum_{i=0}^{T-1} D(F^i(P(n,t+i))) \times M(t)$$

上式のように、解釈変更方法Ｍ（ｔ）をあわせて用いる必要がある。ただし、情報を埋め込んだコンテンツが加工された際には個々の場所Ｐ（ｎ，ｔ）から検出される値Ｄ（Ｐ（ｎ、Ｔ））と、Ｍ（ｔ）との同期をとる必要がある。同期が正しくとれれば埋め込み時と検出時で２回Ｍ（ｔ）が乗ぜられて＋１になるので本来のビット情報が得られる。同期をとる際には、以下の何れかの手法を用いる。

【００９０】

［＋／－反転］

解釈変更方法Ｍ（ｔ）として、Ｍ（ｔ＋１）＝－Ｍ（ｔ）とする。埋め込みビット情報を正しく解釈するためには、まず個々の場所Ｐ（ｎ、ｔ）から検出される値Ｄ（Ｐ（ｎ、ｔ））に対し、隣り合う時間で符号の反転する系列を掛け合わせて検出値Ｄｎを計算する。正しくＭ（ｔ）と同期が取れている場合にはビット情報を正しく検出できるが、同期がとれていない場合には＋／－の符号がすべて反転して各Ｄ（Ｐ（ｎ、ｔ））に掛け合わされるため、反転したビット情報が検出されることになる。そのため、ビットが反転して検出されているか否かを判定する情報Ｗｍを埋め込みビット情報以外に埋め込んでおく。埋め込みビット情報を検出した際に、Ｗｍの符号を見て、

【数３８】

$$D_n = D_n \ (if\ Wm_{bitrev} > 0)$$
$$D_n = -D_n \ (if\ Wm_{bitrev} < 0)$$

と解釈しなおし、埋め込みビット情報を検出する。

【００９１】

［最大検出値の適用］

解釈変更方法Ｍ（ｔ）として、周期Ｔ’を持ち、

【数３９】

$$Conv(j) = \sum_{i=0}^{T'-1} M(t+j+i) \times M(t+i)$$

がｊ＝ｍ＊Ｔ’（ｍは自然数）の時のみ最大値Ｔ’をもつ系列を用意する。検出の際には、Ｍ（ｔ）をシフトして求めたそれぞれの検出値のうち、最大となるシフト量を求めることにより、解釈変更方法Ｍ（ｔ）と同期をとる。

【数４０】

$$D_n = \max_{0 \le j \le T'} \left(\sum_{i=0}^{T'-1} D(F^j(P(n,t+i))) \times M(t+j) \right)$$

【００９２】

[ビット情報以外の情報の利用]

検出したビット解釈Ｍ（ｔ）を他の信号の検出値で与える。例えば、電子透かし検出用にユニットの位置決め情報（シンク情報、Ｓ（ｔ）と表記する)が埋まっている場合には、ビット情報埋め込み時に、その信号の符号をＭ（ｔ）と同符号に反転させておく。検出時にはシンク情報を検出し、その符号をビット解釈に用いる。

【数４１】

$$D_n = \sum_{i=0}^{T-1} D(F^j(P(n,t+i))) \times sin(S(t))$$

【００９３】

【発明の効果】

本発明により、フレーム同期のための信号を埋める必要がない、実用的でかつ

堅牢な電子透かしの方法およびシステムが提供される。またフレーム同期をしないので検出にかかる時間が短くなる。さらにフレーム同期をするために検出システムに必要だった記憶容量が必要ない。悪意のある第３者により埋め込みのアルゴリズムを困難にする電子透かしの方法およびシステムが提供される。

【図面の簡単な説明】

【図１】

本発明の実用的で堅牢な電子透かしの埋め込み方法のフローチャートを示す。

【図２】

本発明の実用的で堅牢な電子透かしの検出方法のフローチャートを示す。

【図３】

時間軸と周波数軸およびビットの埋めこみを説明する図である。

【図４】

フレームの重なりを説明する図である。

【図５】

振幅の増減を説明する図である。

【図６】

窓かけと、フレームの重ねあわせを説明する図である。

【図７】

フレームずれなしの場合を説明する図である。

【図８】

１フレームずれを説明する図である。

【図９】

サイクル同期を説明する図である。

【図１０】

付加情報の半分をより重要な情報であるとして広い周波数帯を割り当てた例である。

【図１１】

斜め埋めを説明する図である。

【図１２】

信頼性の差別化と均等化を説明する図である。

【図１３】

高速化可能な斜め埋めを説明する図である。

【図１４】

埋め込み前の前処理、埋め込み後の後処理を説明する図である。

【図１５】

リサンプリングを行ってから埋め込み信号を計算する方法を説明する図である。

【図１６】

リサンプリングを行ってから埋め込み信号を計算する別の方法を説明する図である。

【図１７】

埋め込み開始ユニットを説明する図である。

【図１８】

仮想的な埋め込み開始位置を説明する図である。

【図１９】

ビット情報埋め込み位置の時間変動例を示す図である。

【図２０】

情報を埋め込まない位置の挿入例を示す図である。

【図２１】

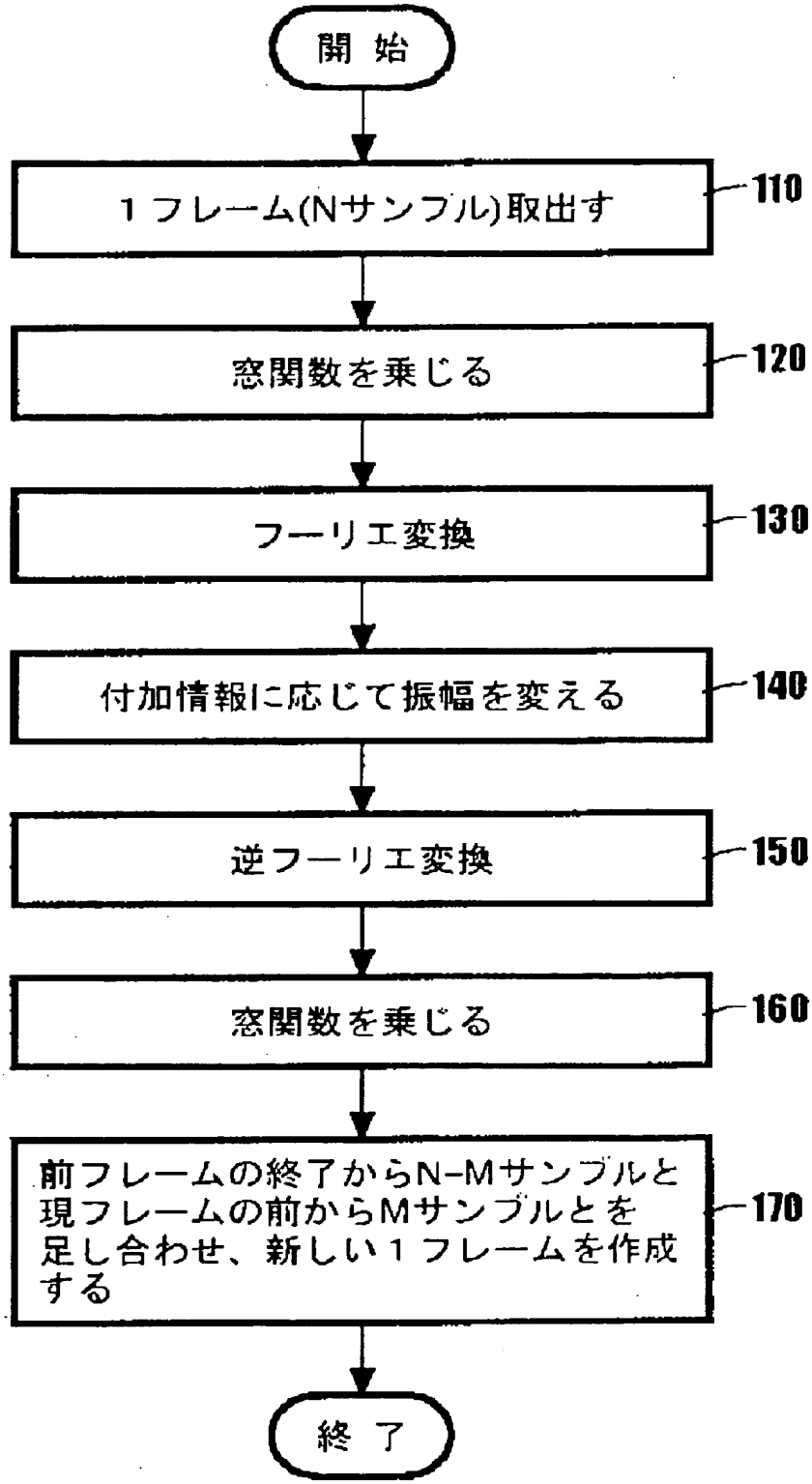
周期２Ｔでビット反転する情報の埋め込み例を示す図である。

【図２２】

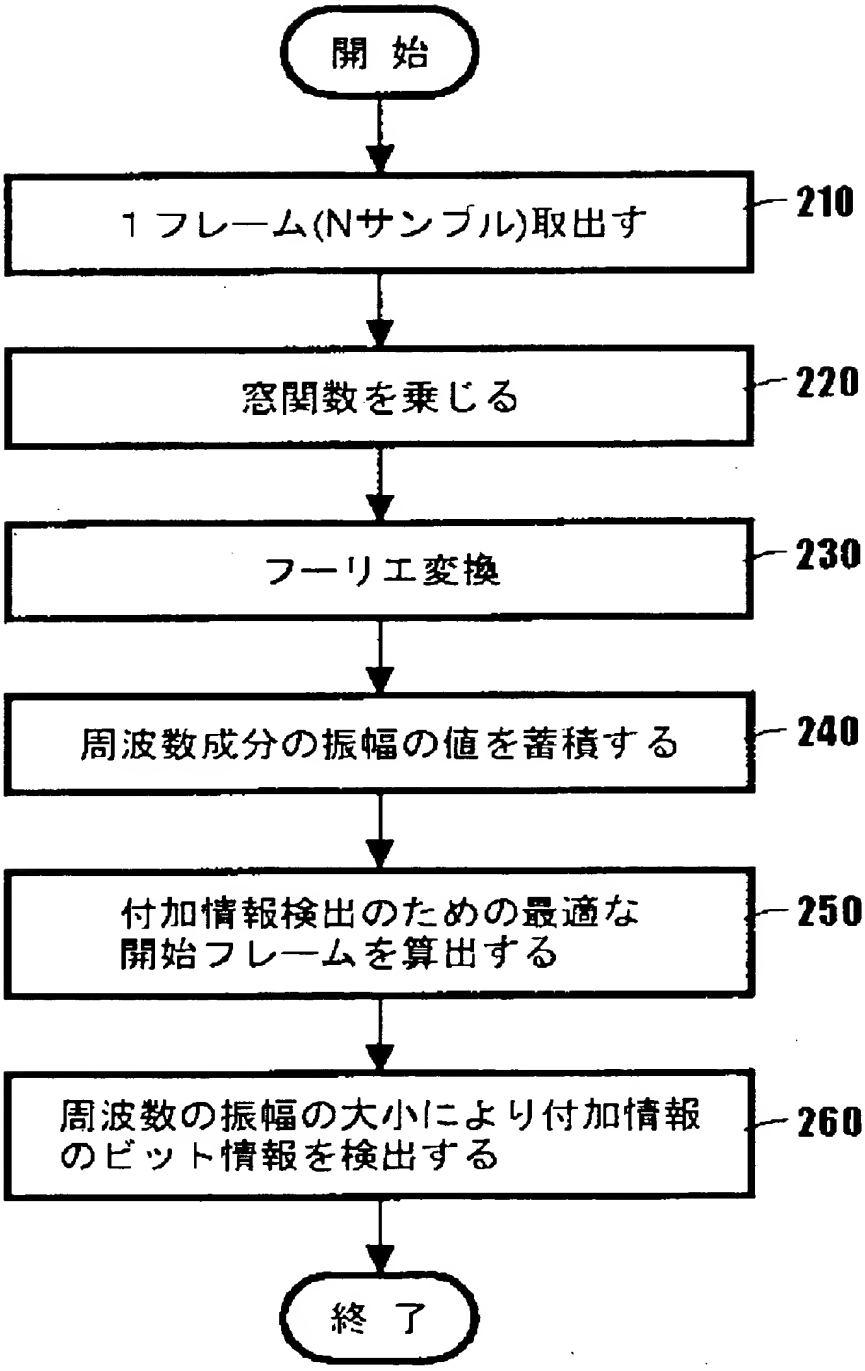
ビット情報以外の情報の利用例を示す図である。

【書類名】　　図面

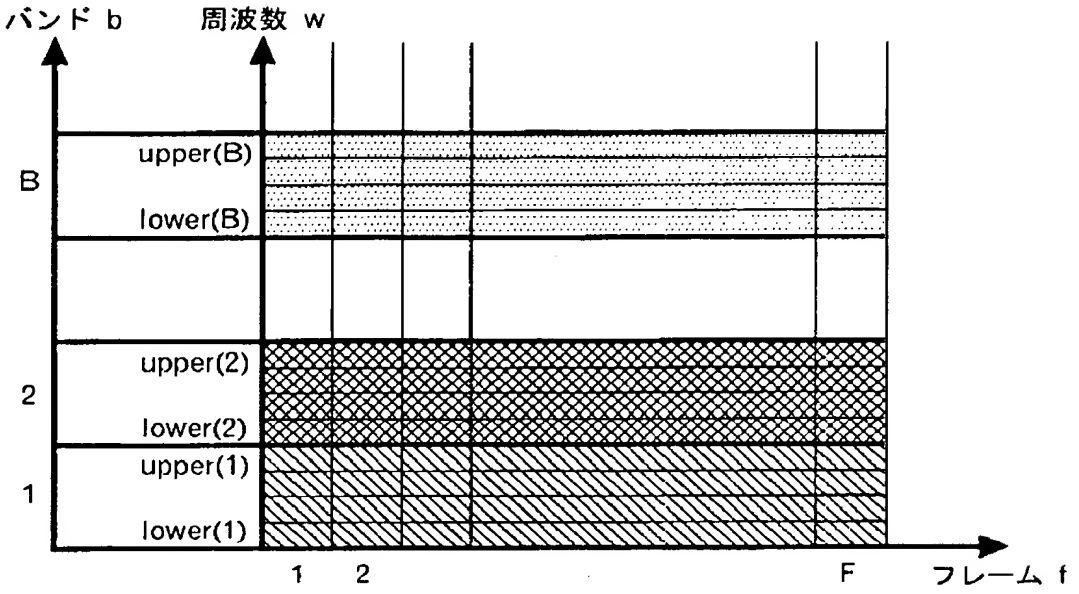
【図１】


開 始
１フレーム(Nサンプル)取出す
110
窓関数を乗じる
120
フーリエ変換
130
付加情報に応じて振幅を変える
140
逆フーリエ変換
150
窓関数を乗じる
160
前フレームの終了からN-Mサンプルと
現フレームの前からMサンプルとを
足し合わせ、新しい１フレームを作成
する
170
終 了

【図２】

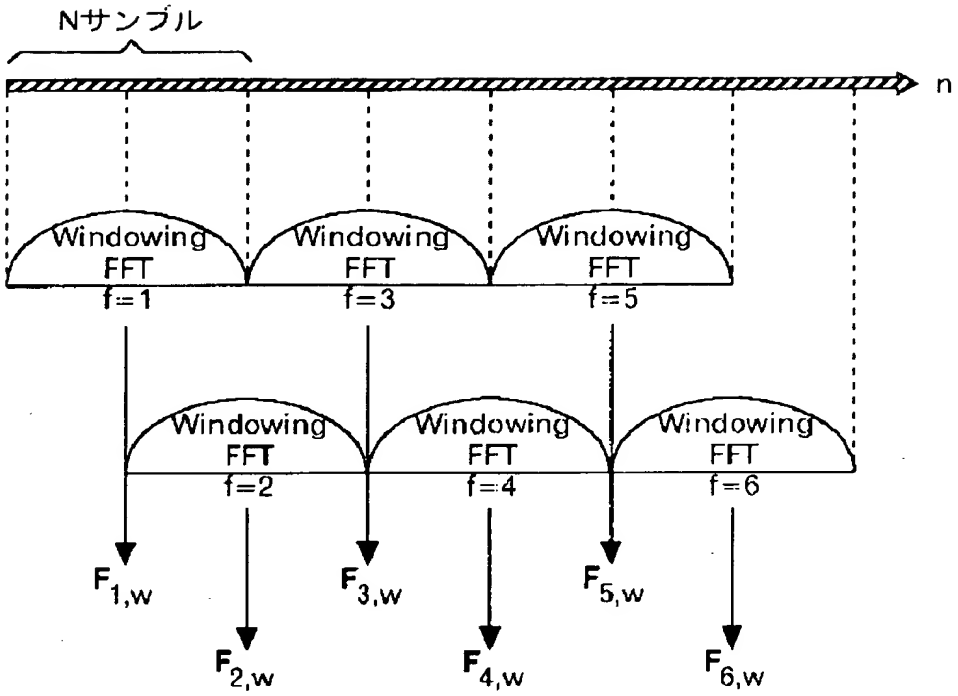

開 始
１フレーム(Nサンプル)取出す
210
窓関数を乗じる
220
フーリエ変換
230
周波数成分の振幅の値を蓄積する
240
付加情報検出のための最適な
開始フレームを算出する
250
周波数の振幅の大小により付加情報
のビット情報を検出する
260
終 了

【図３】


バンド b
周波数 w
B
upper(B)
lower(B)
2
upper(2)
lower(2)
1
upper(1)
lower(1)
1
2
F
フレーム f

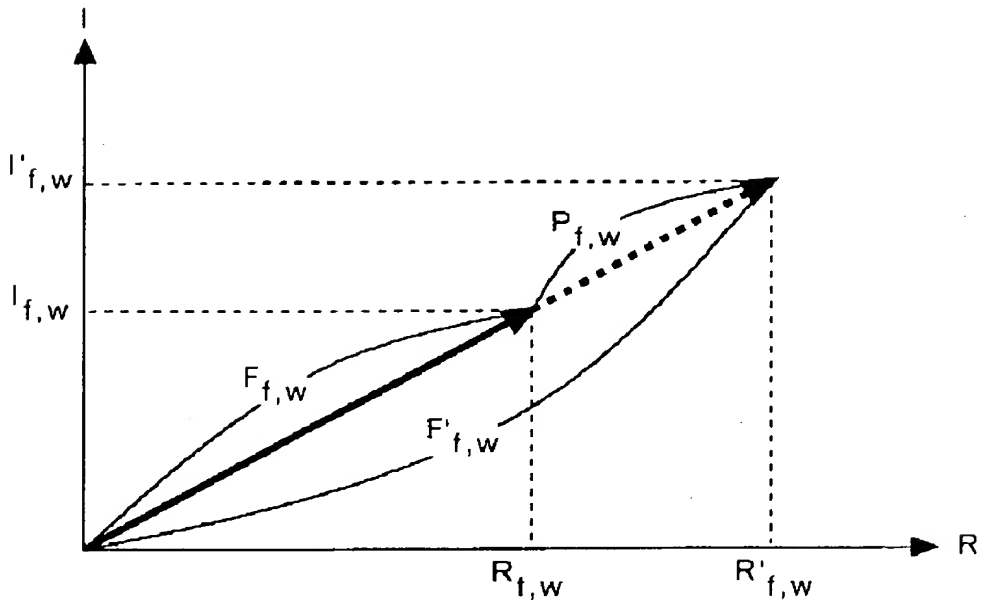
時間軸と周波数軸

【図４】


Nサンプル
n
Windowing FFT f=1
Windowing FFT f=3
Windowing FFT f=5
Windowing FFT f=2
Windowing FFT f=4
Windowing FFT f=6
F1,w
F2,w
F3,w
F4,w
F5,w
F6,w

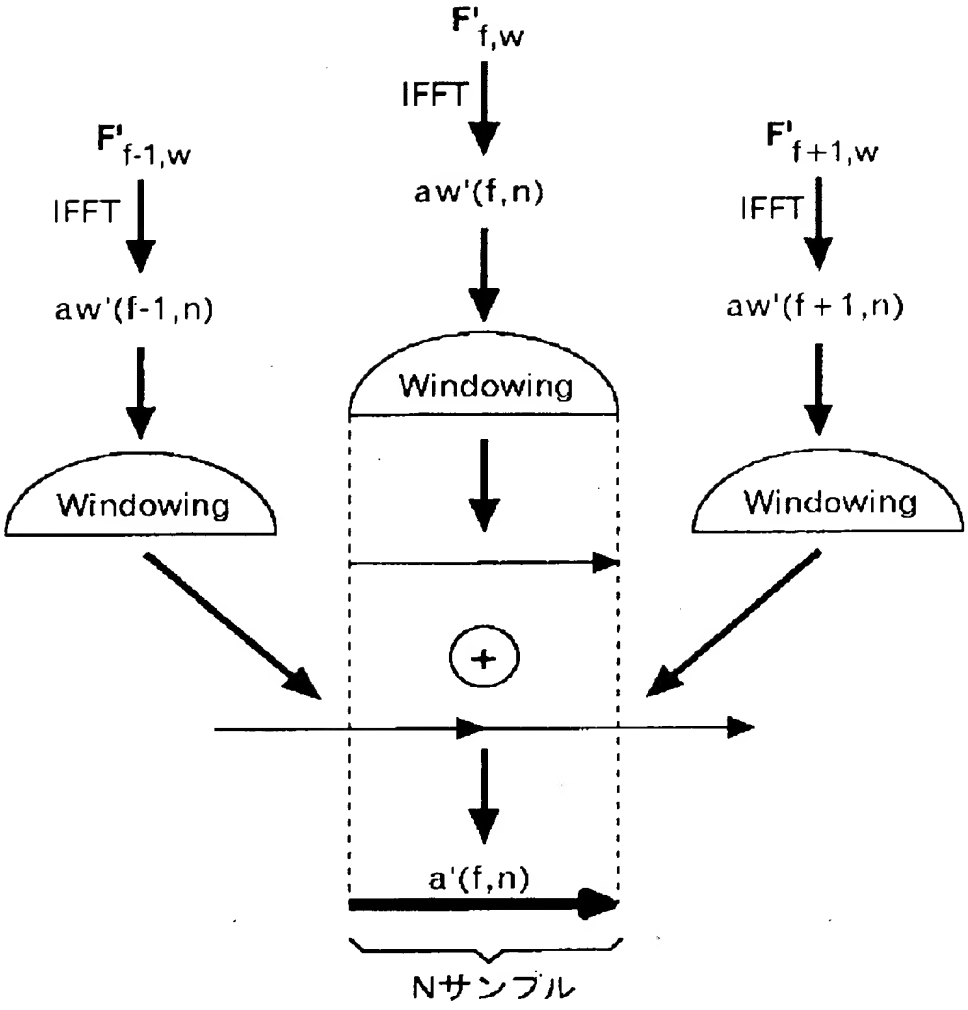
フレーム

【図５】



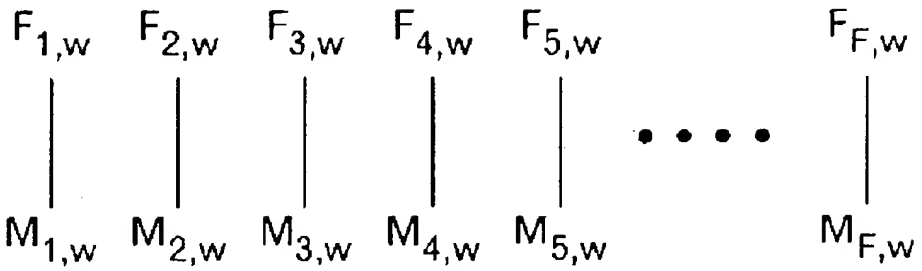
振幅を増減する

【図６】



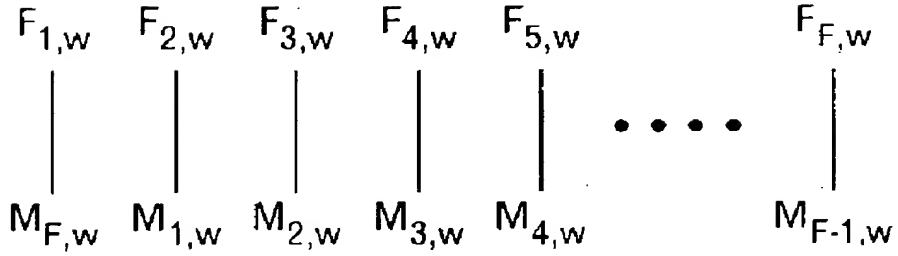
窓をかけ、重ね合わせて時間順に出力

【図７】



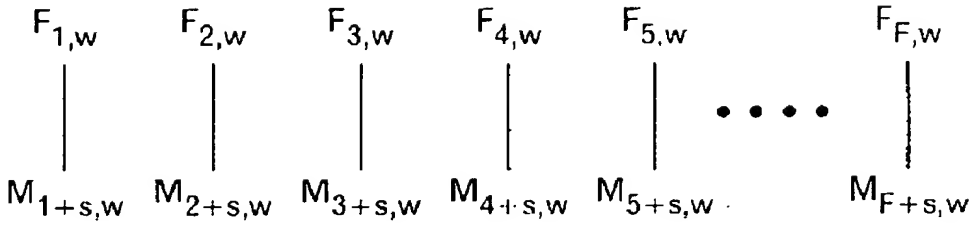
フレームずれなし

【図８】



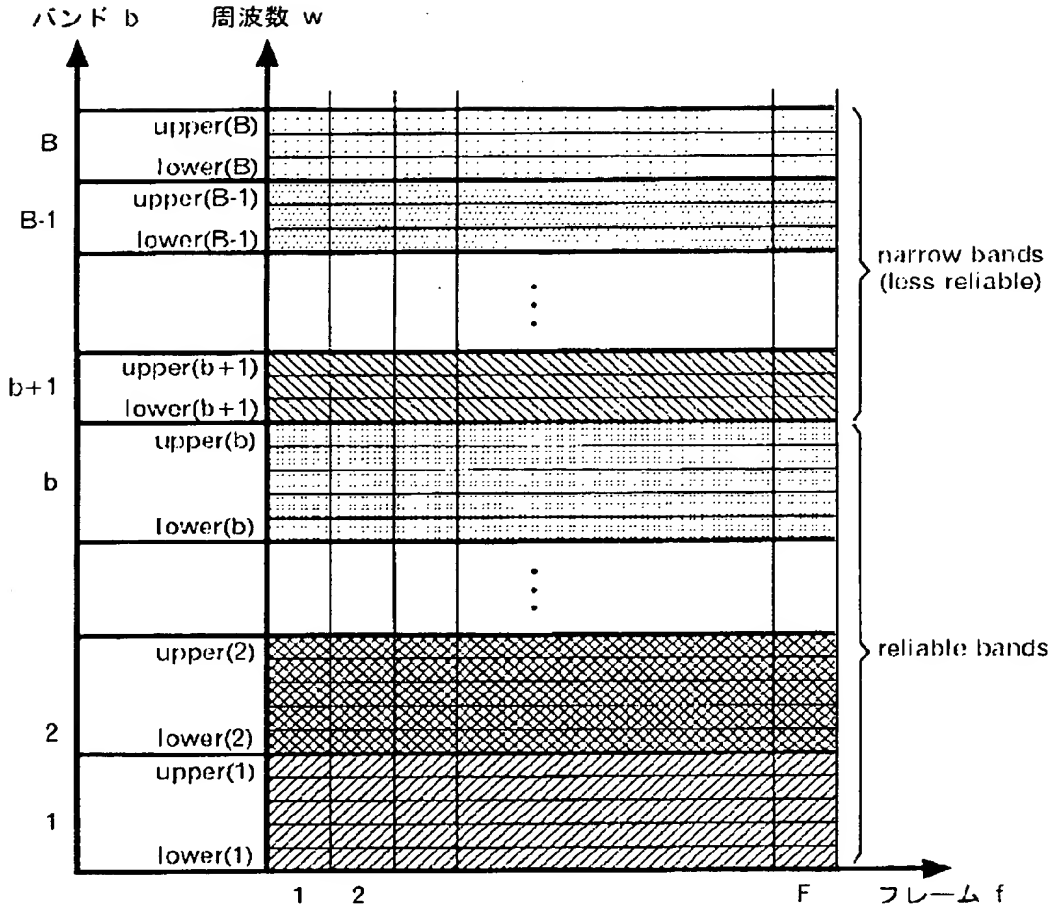
１フレームずれ

【図９】



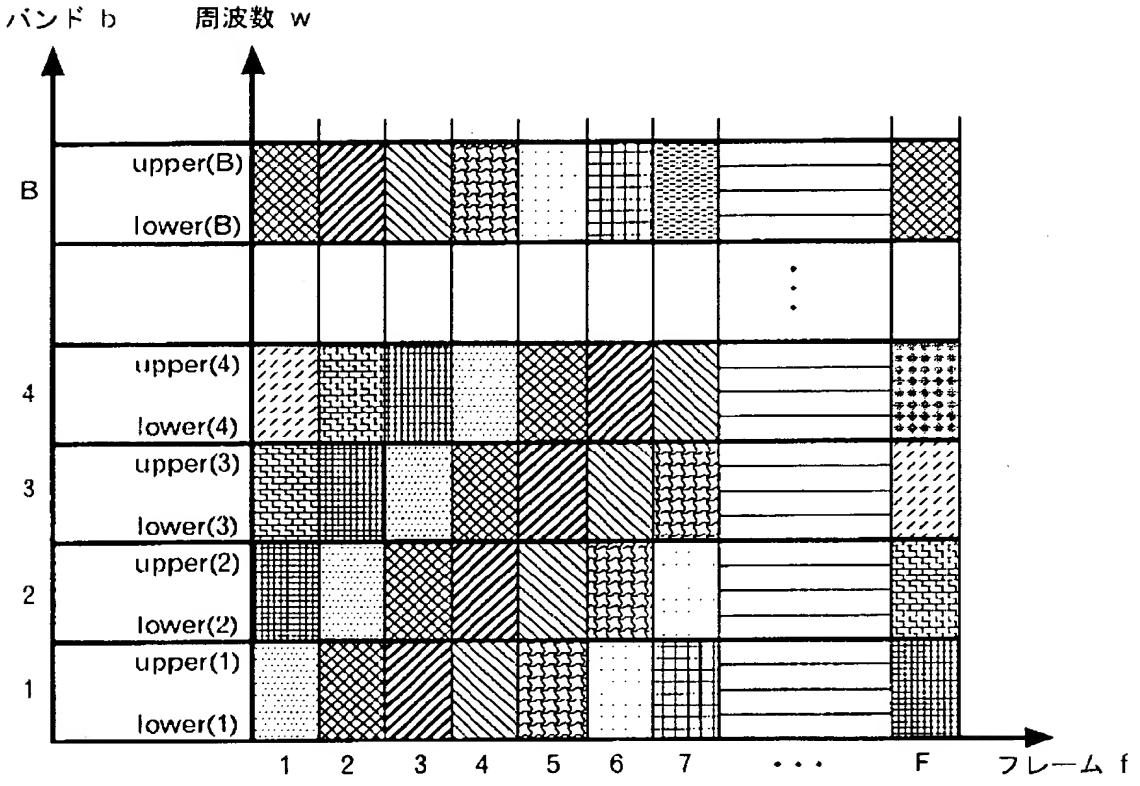
サイクル同期

【図１０】



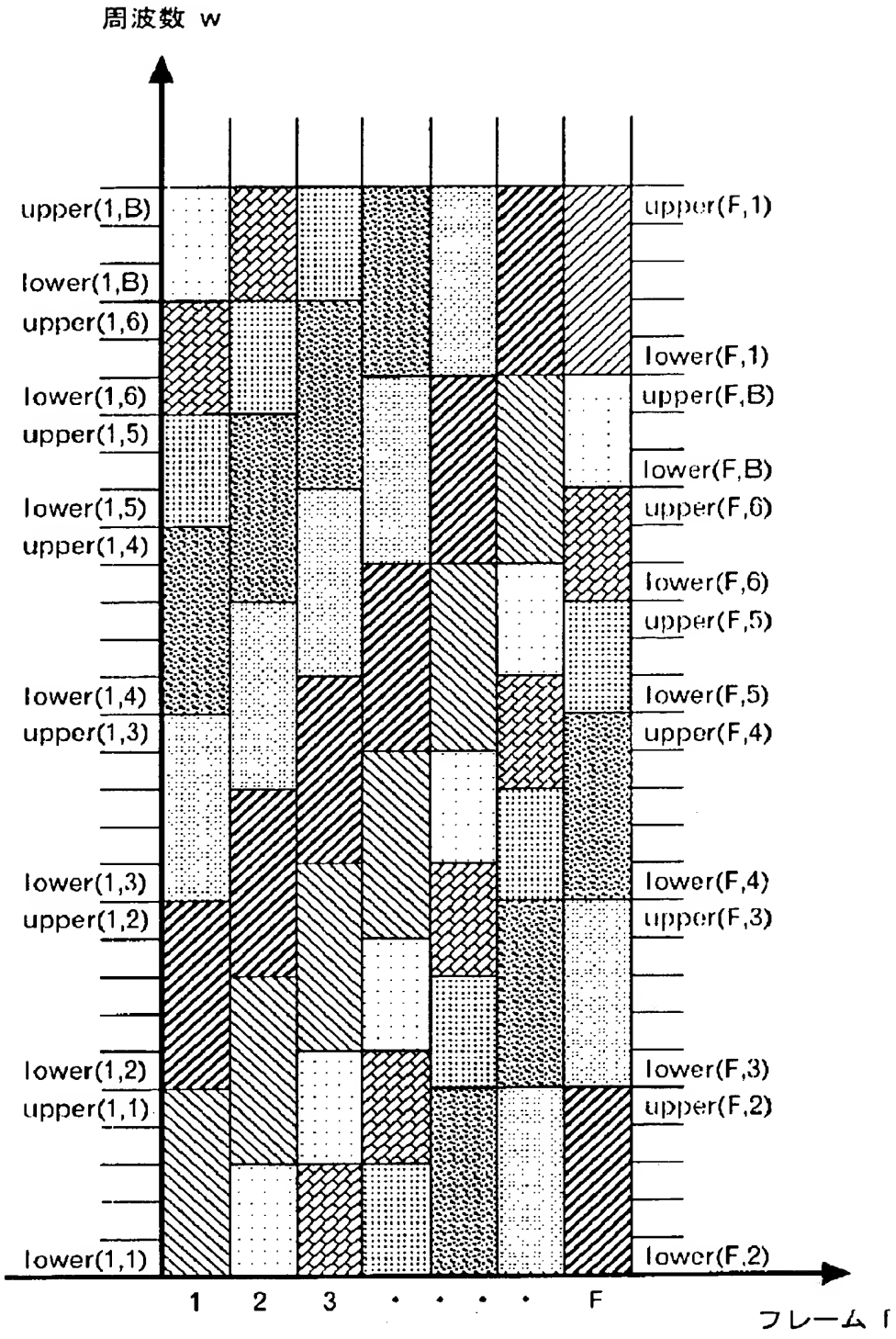
信頼性に差を設ける

【図１１】


バンド b
周波数 w
B
upper(B)
lower(B)
4
upper(4)
lower(4)
3
upper(3)
lower(3)
2
upper(2)
lower(2)
1
upper(1)
lower(1)
1 2 3 4 5 6 7 ・・・ F
フレーム f

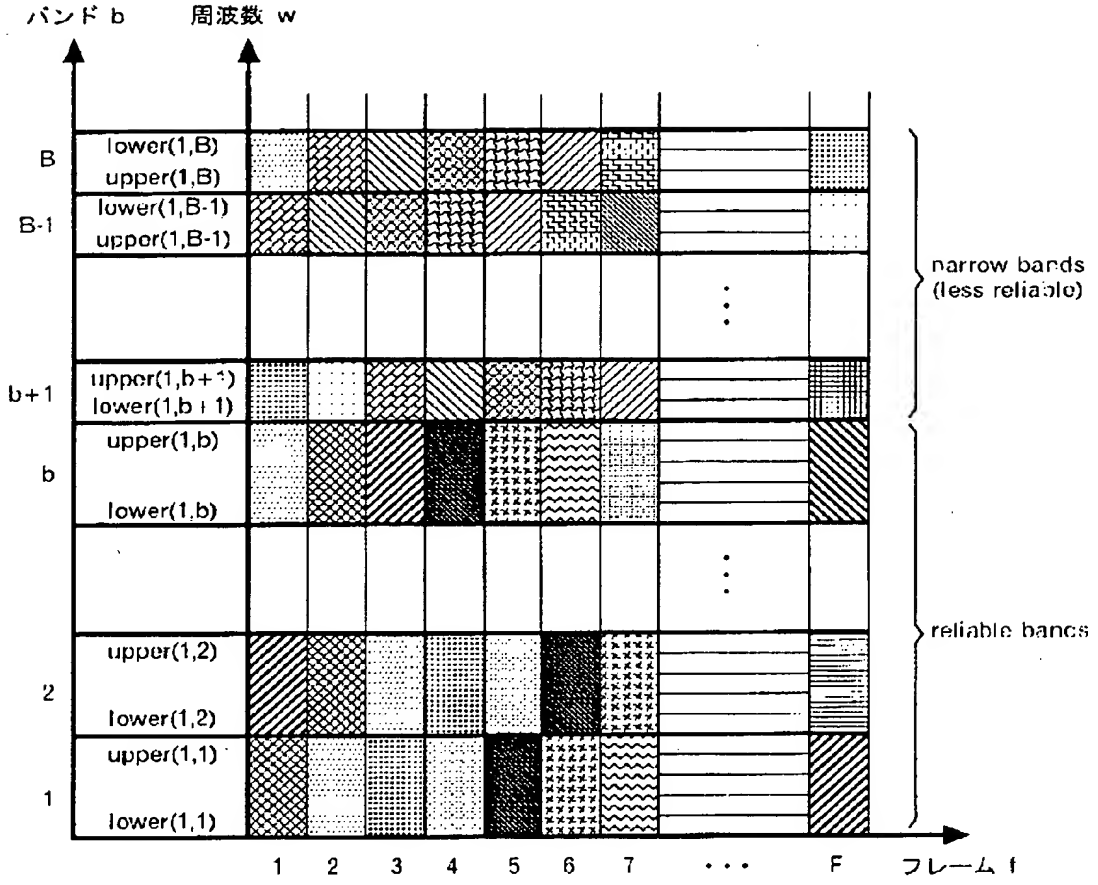
斜め埋め

【図１２】



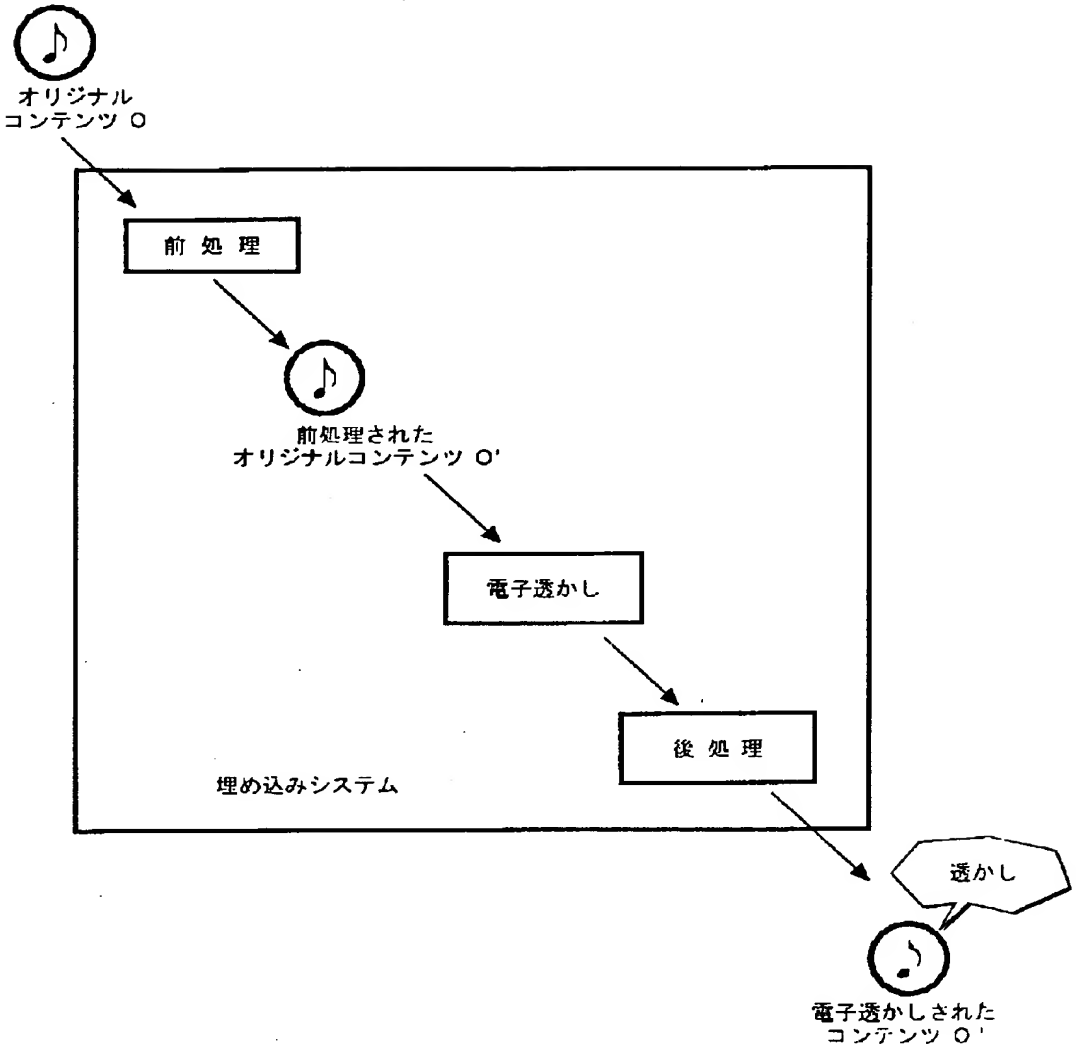
信頼性の差別化と均等化

【図１３】

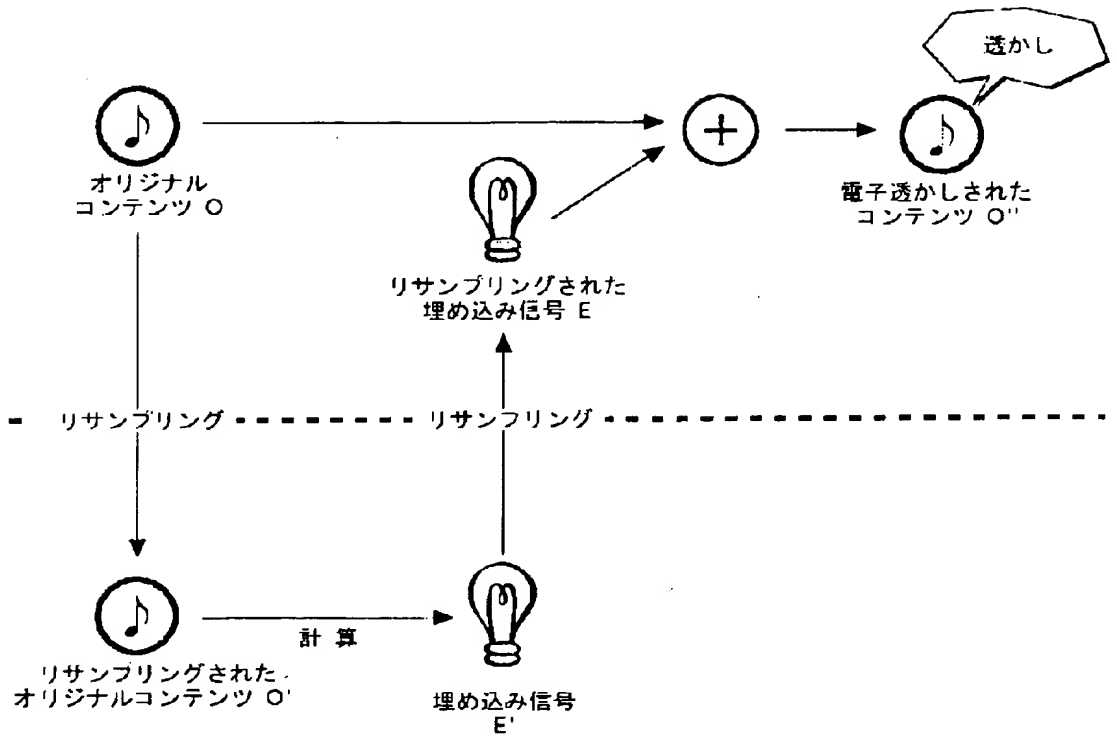


高速化可能な斜め埋め

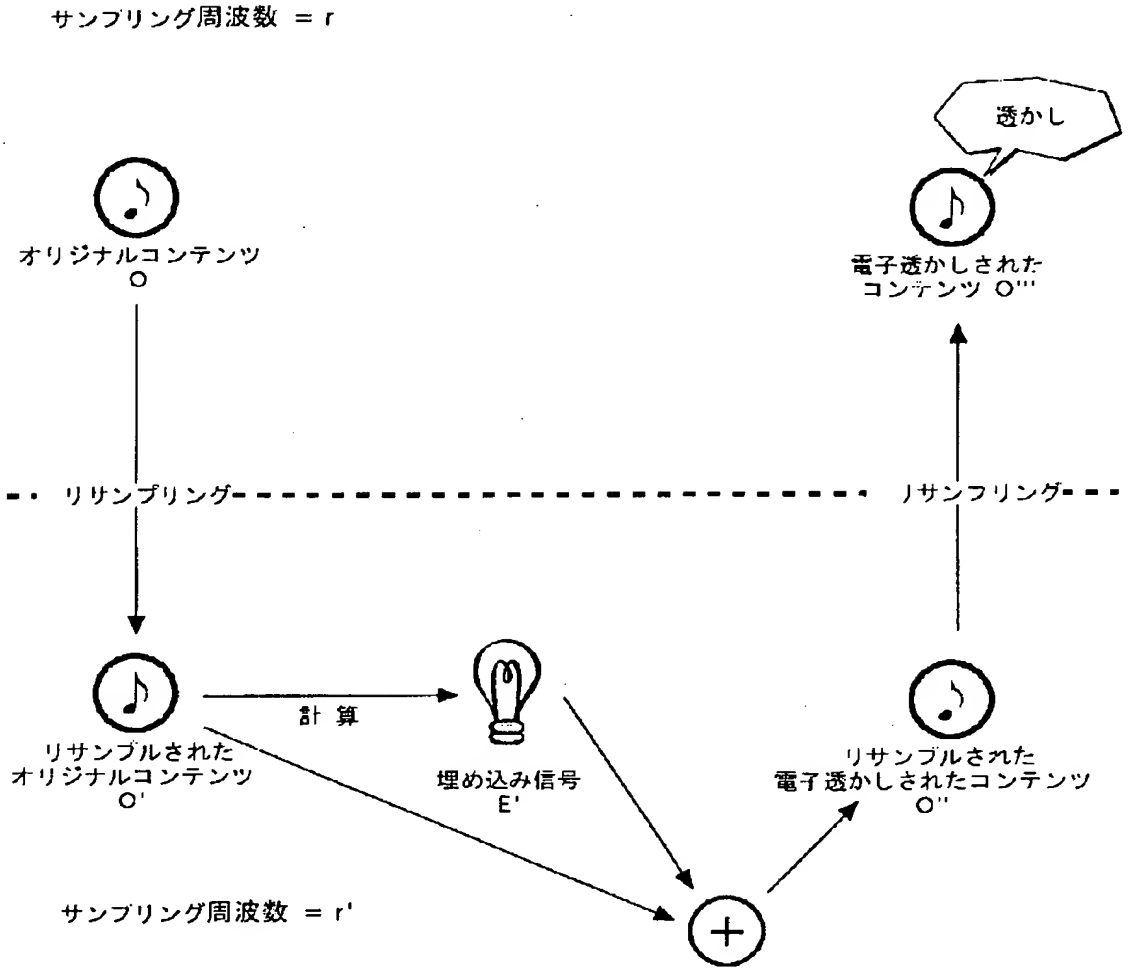
【図１４】


オリジナル
コンテンツ O
前 処 理
前処理された
オリジナルコンテンツ O'
電子透かし
後 処 理
埋め込みシステム
透かし
電子透かしされた
コンテンツ O''

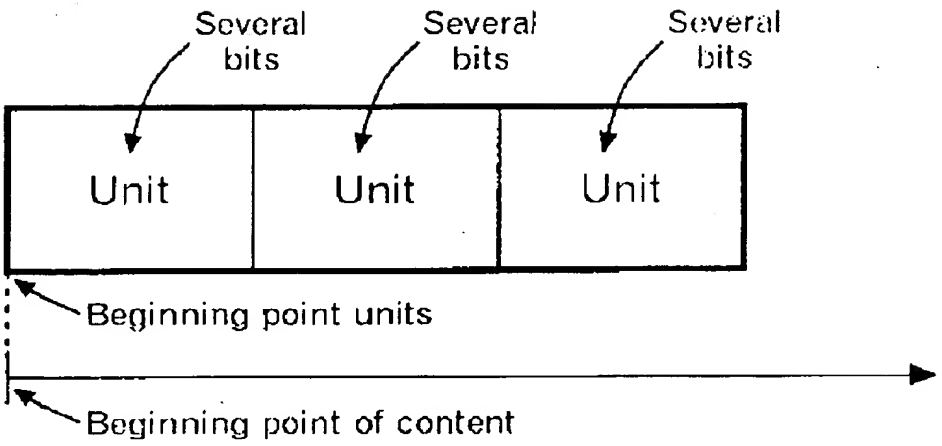
【図１５】


サンプリング周波数 ＝ r
透かし
オリジナル
コンテンツ O
リサンプリングされた
埋め込み信号 E
電子透かしされた
コンテンツ O''
リサンプリング
リサンプリング
計 算
リサンプリングされた
オリジナルコンテンツ O'
埋め込み信号
E'
サンプリング周波数 ＝ r'

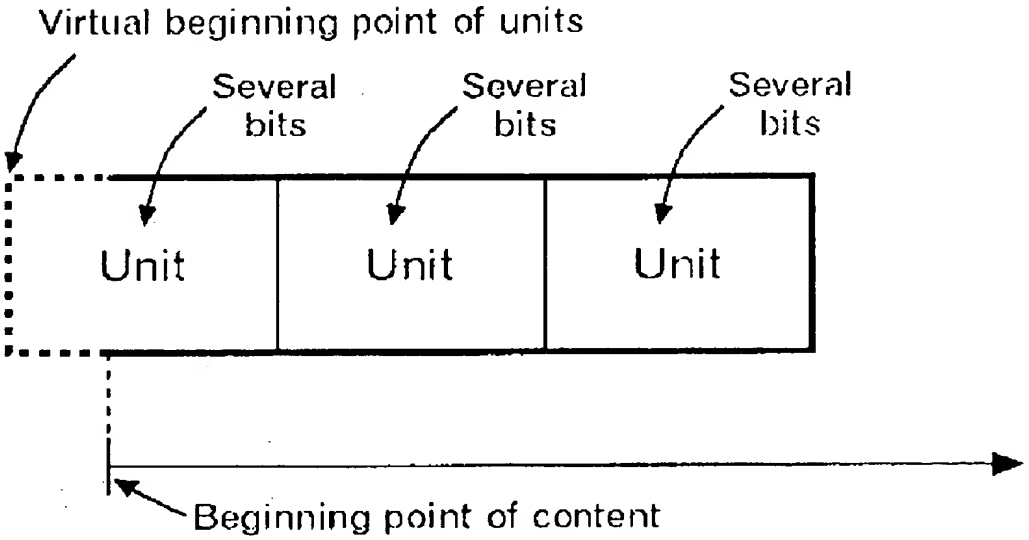
【図１６】


サンプリング周波数 ＝ r
透かし
オリジナルコンテンツ
O
電子透かしされた
コンテンツ O'''
リサンプリング
リサンプリング
計 算
リサンプルされた
オリジナルコンテンツ
O'
埋め込み信号
E'
リサンプルされた
電子透かしされたコンテンツ
O''
サンプリング周波数 ＝ r'

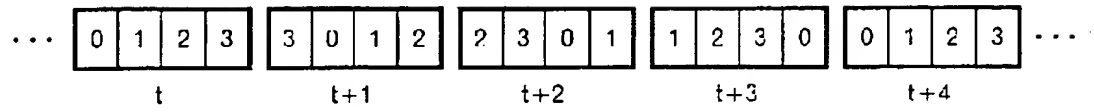
【図１７】


Several bits
Several bits
Several bits
Unit
Unit
Unit
Beginning point units
Beginning point of content

【図１８】

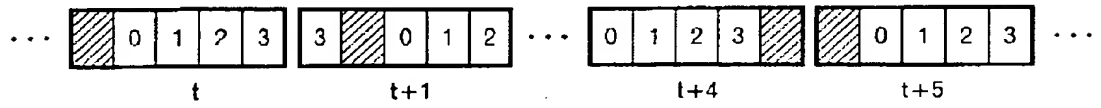

Virtual beginning point of units
Several bits
Several bits
Several bits
Unit
Unit
Unit
Beginning point of content

【図１９】



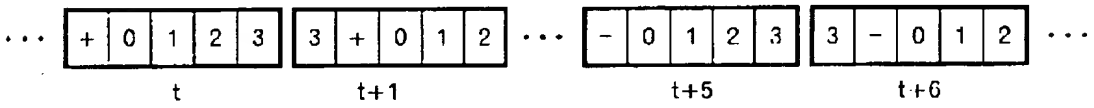
ビット情報埋め込み位置の時間変動例

【図２０】



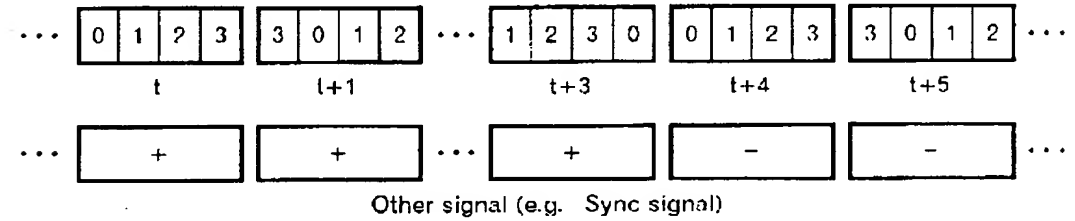
情報を埋め込まない位置の挿入

【図２１】



周期2Tでビット反転する情報の埋め込み

【図２２】



ビット情報以外の情報の利用

【書類名】　要約書

【要約】

【課題】

実用的かつ堅牢な電子透かしの方法およびシステムを提供することである。

【解決手段】

デジタルデータに付加情報を埋め込む、電子透かしシステムであって、１フレームはデジタルデータから取り出したＮ個のサンプルとして構成され、次フレームは前フレームとＭ（０＜Ｍ≦Ｎ／２）サンプル重なるよう定義することを特徴としており、該システムが、デジタルデータから取り出したフレームに窓関数を乗じた後、フーリエ変換を行い、デジタルデータの周波数成分を求める、周波数領域変換部と、周波数領域変換部において得られたデジタルデータの周波数成分の振幅を、付加情報のビット情報と、前記周波数成分の周波数帯により増減する、周波数領域埋め込み部と、周波数領域埋め込み部で得られた、振幅を増減された周波数成分を、逆フーリエ変換を使って時間領域の信号へと戻す、時間領域変換部と、時間領域変換部で得られた時間領域の信号に、窓関数を乗じ、重なり合う前後のフレームを重ね合わせて、付加情報の埋め込まれたフレームを作成する、付加情報埋め込みフレーム作成部を有する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－１９６３９６
受付番号	５００００８１７１０５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　６月３０日

＜認定情報・付加情報＞

【提出日】　平成12年 6月29日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション